PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-041170

(43)Date of publication of application : 08.02.2002

(51)Int.Cl. G06F 1/00
G06F 12/14

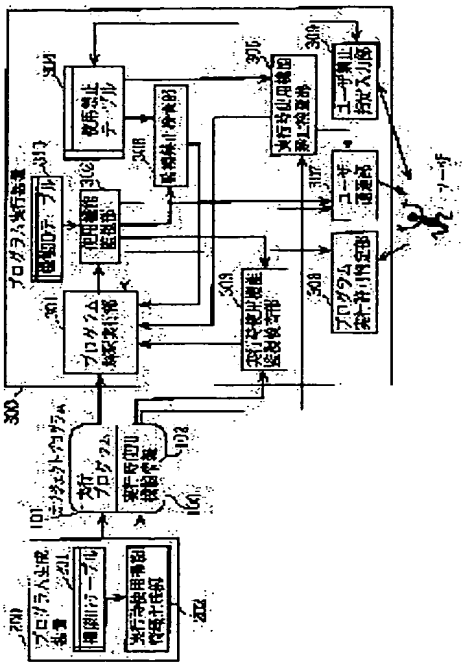
(21)Application number : 2000-227840

(22)Date of filing : 27.07.2000

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(72)Inventor : KANAMARU TOMOKAZU
WAKE HIROYUKI
TOMINAGA NOBUTERU
HARUNA NAOSUKE

(54) PROGRAM PERFORMANCE CONTROLLER



(57)Abstract:

PROBLEM TO BE SOLVED: To provide a means for easily assuring security at the time of performing a downloaded program.

SOLUTION: A program performing device 300 mounted on a portable telephone set acquires a performance program 101 to which performance time the function information 102 declaring a function to be used is added from a communication passage, and allows a program interpretation performing part 301 to successively execute the performance program. At the time of performing the performance program 101, the program performing device 300 stops the performance when the sue of any function included in a user inhibition table 304 indicating any function whose use is inhibited is declared by the performance time use function information 102. Also, the program performing device 300 monitors an instruction to be performed the next during the performance of the performing program 101, and stops the performance when the use of any function used by the instruction is not declared by the performance time use function information 102.

CLAIMS

[Claim(s)]

[Claim 1] It is carried in the device and the program to which the use functional information which shows the function which oneself uses among the functional groups using the specific resource of said device was added is acquired. An acquisition means to be the program execution control unit to perform and to acquire a program from a channel, An activation means to perform the acquired program, and a judgment based on said use functional information are made. The program execution control unit characterized by having the means for stopping which stops the program execution by said activation means in a case predetermined [showing the decision result of program execution being unsuitable].

[Claim 2] Said program is that to which said activation means executes the instruction in said program including two or more instructions. Said means for stopping The instruction which becomes a degree in the program under activation for activation is supervised. The program execution control unit according to claim 1 characterized by stopping said program execution by said activation means when it is the instruction which uses the function by which said instruction is not shown as a function used in said use functional information among said functional groups.

[Claim 3] It is the program execution control unit according to claim 2 which said use functional information is enciphered and is characterized by said means for stopping decoding and referring to said use functional information.

[Claim 4] It is the program execution control unit according to claim 1 said program execution control unit has a prohibition functional storage means memorize the prohibition functional information which shows the function forbid use, and carry out [stopping the program execution by said activation means, when the function of forbidding the use said means for stopping is indicated to be to said prohibition functional information is shown as a function use it to said use functional information, and] as the description.

[Claim 5] The program execution control unit according to claim 4 characterized by including the function of radio in the function to forbid the use which said prohibition functional information shows, at least.

[Claim 6] The program execution control unit according to claim 4 characterized by including the function of the data output from an output device in the function to forbid the use which said prohibition functional information shows, at least.

[Claim 7] The program execution control unit according to claim 4 characterized by including the function of the data acquisition from an input device in the function to forbid the use which said prohibition functional information shows, at least.

[Claim 8] Said program execution control unit is a program execution control unit given in any 1 term of claims 4-7 characterized by having a prohibition functional modification means

to receive actuation of a user and to update said prohibition functional information further according to said actuation.

[Claim 9] An acquisition means to be the program execution control unit which acquires and performs the program which is carried in a Personal Digital Assistant equipped with the memory which has an individual humanity news field, and consists of two or more instructions, and to acquire a program from a channel, An activation means to perform the acquired program, and the program under activation supervise the instruction which it is going to execute next. The program execution control unit characterized by having the means for stopping which stops said program execution by said activation means when said instruction is an instruction which performs data read-out from said individual humanity news field.

[Claim 10] An acquisition means to be the program execution control unit which acquires and performs the program which is carried in a Personal Digital Assistant equipped with the memory which has an individual humanity news field, and consists of two or more instructions, and to acquire a program from a channel, An activation means to perform the acquired program, and the program under activation supervise the instruction which it is going to execute next. The program execution control unit characterized by having the means for stopping which stops said program execution by said activation means when said instruction is an instruction which performs the data store to said individual humanity news field.

[Claim 11] An acquisition means to be the program execution control unit which acquires and performs the program which is carried in a Personal Digital Assistant and consists of two or more instructions, and to acquire a program from a channel, An activation means to perform the acquired program, and the program under activation supervise the instruction which it is going to execute next. The program execution control unit characterized by having the means for stopping which stops said program execution by said activation means when it is the instruction which calls the functional manipulation routine to which said instruction is the functional manipulation routine with which said Personal Digital Assistant is equipped, and communicates with the exterior of said Personal Digital Assistant.

[Claim 12] Said functional manipulation routine is a program execution control unit according to claim 11 characterized by being the functional manipulation routine which performs data transmission to the exterior of said Personal Digital Assistant.

[Claim 13] An acquisition means to be the program execution control unit which acquires and performs the program which is carried in a Personal Digital Assistant and consists of two or more instructions, and to acquire a program from a channel, An activation means to perform the acquired program, and the program under activation supervise the instruction which it is going to execute next. The means for stopping which stops said program execution by said activation means when said instruction is the functional manipulation routine with which said Personal Digital Assistant is equipped and it is the instruction which calls the functional

manipulation routine which performs data output from the output device with which said Personal Digital Assistant is equipped The program execution control unit characterized by having.

[Claim 14] An acquisition means to be the program execution control unit which acquires and performs the program which is carried in a Personal Digital Assistant and consists of two or more instructions, and to acquire a program from a channel, An activation means to perform the acquired program, and the program under activation supervise the instruction which it is going to execute next. The means for stopping which stops said program execution by said activation means when said instruction is the functional manipulation routine with which said Personal Digital Assistant is equipped and it is the instruction which calls the functional manipulation routine which performs data acquisition from the input device with which said Personal Digital Assistant is equipped The program execution control unit characterized by having.

[Claim 15] Said program execution control unit is a program execution control unit given in any 1 term of claims 1-14 further characterized by having a notice means to notify a user of the stopped purport when said program execution stops by said means for stopping.

[Claim 16] Said program execution control unit is a program execution control unit given in any 1 term of claims 1-15 further characterized by having a halt discharge means to receive the input by the user and to cancel a halt according to said input when said program execution stops by said means for stopping.

[Claim 17] Program execution control processing in which the object program with which the use functional information which shows the function which oneself uses among the functional groups using the specific resource of said device in the device which has a program execution function was added is acquired and performed It is the record medium which recorded the control program made to perform. Said program execution control processing The acquisition step which acquires an object program from a channel, and the execute step which performs the acquired object program, The record medium characterized by having the halt step which stops activation of an object program in the predetermined case which makes a judgment based on said use functional information, and expresses that the activation whose decision result is an object program is unsuitable.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the technique for the security reservation in the case of downloading the application program for Personal Digital Assistants, and performing on a Personal Digital Assistant especially, about the technique which prevents the

damage by inaccurate program execution.

[0002]

[Description of the Prior Art] In order to realize a household-electric-appliances device, the escape of the function of a Personal Digital Assistant ("henceforth a household-electric-appliances device etc."), etc. by making progress of communication technology, software skill, etc. into a background in recent years, the request of the researches and developments about distribution service of a program to the household-electric-appliances device by which CPU was incorporated is increasing.

[0003] If a household-electric-appliances device etc. is equipped with the function corresponding to distribution service of a program, a household-electric-appliances device etc. can download the application program prepared for the server on an external network, and when required, it can perform the application program. Therefore, users, such as a household-electric-appliances device, can use the function of the versatility added by download not only from the function made from the beginning by the household-electric-appliances device etc. but from after, for example, it enables a user to choose, download and use for arbitration the application program which realizes the function which self desires etc.

[0004] For example, various application programs, such as an application program of the function which related to a message and communication facility closely as an object of the distribution service to a Personal Digital Assistant, and an address book, a game, can be considered. The application program set as the object of distribution service is fundamentally created by the manufacturer who is manufacturing the household-electric-appliances device etc., its related company, etc. Moreover, also when created by ordinary program development persons and companies which received distribution of the tools it is incomparable to the development environment of the application program for specific devices from manufacturers, such as a household-electric-appliances device, etc., it thinks.

[0005] In this way, an assumption of the case where the application program created by the person of a manufacturer and others is downloaded and used by sides, such as a household-electric-appliances device, needs to equip the household-electric-appliances device with the function for security reservation. It is because it cannot say that there is nothing also when the application program which may be unjustly changed by the person with the malicious application program created by the manufacturer etc. as a just thing so that actuation which is not desirable may be performed, and performs actuation which is not desirable by ordinary program development persons etc. is offered.

[0006] As actuation by the application program which is not desirable, there is actuation which updates freely the data in the data storage area in a device, and read-out of the information (henceforth "individual humanity news") in connection with the privacy of the telephone number memorized inside in Personal Digital Assistants, such as a portable telephone, and a mail address and others, the call origination to the exterior, etc. can be called

actuation which is not desirable when it does not meet a user's intention.

[0007] By the way, in fields, such as a personal computer, there is a device of the code verifier of a Java (trademark) virtual machine conventionally as structure which realizes the security reservation at the time of activation of the application program downloaded from the Internet. Before it carries out interpretation activation of the Java class file which is an application program, a code verifier inspects the format and instruction train, and while the downloaded Java class file performs according to static constraint or structure constraint, it guarantees not performing dangerous actuation. This code verifier is described in detail by "The Java Virtual Machine Specification" (Tim Lindholm, Frank Yellin work, Addison-Wesley, 1997).

[0008]

[Problem(s) to be Solved by the Invention] However, since inspection of the justification of the application program by this code verifier is complicated processing, it requires a great processing step. Therefore, in order to perform a Java class file, also at the lowest, expensive computer resources, such as CPU of high performance 100MHz or more and an availability of the big memory of 2MByte(s) - 4MByte, are needed for a clock frequency. Since this is the excessive amount of resources for most household-electric-appliances devices etc. in current, it does not become the means of security reservation realistic for a household-electric-appliances device etc. to have a code verifier.

[0009] Then, this invention is made in view of aiming at the security reservation at the time of a household-electric-appliances device etc. downloading the application program made into the object of distribution service towards the household-electric-appliances device etc., and performing it, and aims a household-electric-appliances device etc. at offering the program execution control unit which realizes the security reservation at the time of downloading and performing an application program by the comparatively simple approach so that it can apply to especially a Personal Digital Assistant.

[0010]

[Means for Solving the Problem] In order to solve the above-mentioned technical problem, the program execution control unit concerning this invention It is carried in the device and the program to which the use functional information which shows the function which oneself uses among the functional groups using the specific resource of said device was added is acquired. An acquisition means to be the program execution control unit to perform and to acquire a program from a channel, It is characterized by having the means for stopping which stops the program execution by said activation means in the predetermined case which makes a judgment based on said use functional information, and expresses that the decision result of program execution is unsuitable as an activation means to perform the acquired program.

[0011] Since the use functional information which shows beforehand the function which that program uses for a program by the above-mentioned configuration is added, it becomes possible by using this use functional information to secure security by the comparatively simple approach. Namely, it can realize [whether the program uses the function in which use

should be forbidden, and] now by the configuration with simple detecting detecting that the program is altered and by referring to use functional information by comparing use functional information with actuation of an actual program.

[0012]

[Embodiment of the Invention] Hereafter, the program execution equipment which is the gestalt of operation of this invention is explained.

<Configuration> drawing 1 is the block diagram of the program execution equipment 300 grade concerning the gestalt of operation of this invention.

[0013] The object program 100 performed in program execution equipment 300 and the program generation equipment 200 which generates an object program 100 are shown in this drawing besides the program execution equipment 300 with which a portable telephone is equipped.

<Program generation equipment> program generation equipment 200 is equipment which generates the object program which added execution-time use functional information, and is the compiler and linker which operate on a computer. This object program means the program of the execute form which operates on program execution equipment 300, and is an application program. In addition, about execution-time use functional information, it mentions later.

[0014] Program generation equipment 200 has the function which generates execution-time use functional information in addition to a function equivalent to the conventional compiler and a linker, and in order to realize the function which generates execution-time use functional information, it is equipped with the function ID table 201 and the execution-time use functional information generation section 202. Drawing 3 is drawing showing the DS and the example of contents of a function ID table.

[0015] A function ID table is a table which consists of a set of the group of a function ID 401 and the library number 402. In the example of contents shown in this drawing, the library number [function / ID / of 0x0001] 6 is matched. Here, a function ID 401 is the identifier of each function which the object program which operates on program execution equipment 300 uses. In addition, classification arrangement of each function in which the object program which operates on program execution equipment 300 as a premise on employment can be used is carried out beforehand, and suppose that the identifier is set to each.

[0016] Moreover, the library number 402 is a number of the library program which can be called within an object program. That is, it is the number of the library program prepared on the program execution equipment 300 which is the operating environment of an object program. In addition, the function which can be used by library call has the data output function for example, to a wireless interface, the data output function to a display, the data output function to a voice output circuit, a data input function from a wireless interface, a data input function from a carbon button, etc. In the example of contents of drawing 3 , the function which Function ID means is written in addition for convenience in a parenthesis.

[0017] After program generation equipment 200 generates an object program by the function equivalent to the conventional compiler and a linker, the execution-time use functional information generation section 202 generates the execution-time use functional information which shows the function which an object program uses, and adds to the object program by searching the library program currently called in the generated object program, and obtaining a function ID in the light of the function ID table 201.

[0018] Drawing 4 is drawing showing the DS and the example of contents of execution-time use functional information which are added to an object program. Execution-time use functional information is the information which matched the flag 502 which shows whether the object program which actually serves as an addition place of the information for every function ID is using it about all the functions that an object program can use by library call. A flag 502 shows the purport which 0x00 does not use, and shows the purport which 0x01 uses.

[0019] As for the example of contents of this drawing, for example, the function ID is not used, as for the function of 0x0001, but, as for the function of 0x0002, Function ID shows that it is used. The object program 100 generated by such program generation equipment 200 consists of an executive program 101 and execution-time use functional information 102, as shown in drawing 1 . Here, an executive program 101 is the usual object program itself, and interpretation activation is carried out on program execution equipment 300.

[0020] An object program 100 is for example, a Java class file, and the execution-time use functional information 102 is placed as attribute information into a Java class file. In addition, a Java class file can add attribute information. Moreover, attribute information can set up an identification number and can define the contents according to the agreement between specific Java virtual machines. That is, it is possible to build a Java virtual machine so that the attribute information on a specific identification number can be interpreted. Moreover, by the specification of a Java virtual machine, the Java virtual machine which cannot interpret attribute information on the specific identification number is supposed that the attribute information is skipped.

[0021] Here, when program execution equipment 300 acquired and performs an object program 100 and you load the execution-time use functional information 102 to memory, suppose that it is it what may be referred to by program execution equipment 300.

It has <program execution equipment> program execution equipment 300 in a portable telephone, and it is equipment which acquires and performs an object program 100, and contains an operating system and a Java virtual machine.

[0022] Program execution equipment 300 has the program interpretation activation section 301, the use functional Monitoring Department 302, the execution-time use functional monitor Banking Inspection Department 303, the disable table 304, the execution-time use functional prohibition Banking Inspection Department 305, the monitor prohibition Banking Inspection Department 306, the user notification section 307, the program execution authorization judging section 308, the user prohibition assignment input section 309, and the

function ID table 310, as shown to drawing 1 . Each part of these programs interpretation activation section 301 others demonstrates the function by performing the control program with which the memory of a portable telephone was equipped fundamentally by CPU.

[0023] Here, the program interpretation activation section 301 is the so-called interpreter which carries out interpretation activation of the executive program 101, and carries out interpretation activation of the Java class file serially like the conventional Java virtual machine fundamentally. however, the function as an interpreter usual in the program interpretation activation section 301 -- in addition, it has the function in which interpretation activation can be suspended, by receiving a notice of the execution-time use functional monitor Banking Inspection Department 303, the execution-time use functional prohibition Banking Inspection Department 305, or the monitor prohibition Banking Inspection Department 306 during interpretation activation of an executive program 101.

[0024] While the program interpretation activation section 301 is carrying out interpretation activation of the executive program 101, the use functional Monitoring Department 302 supervises the Java cutting tool code (henceforth "an instruction") which is going to be performed next, and when either tends to be used among the functions defined beforehand, it outputs the function ID about the function which was going to be used. That is, the use functional Monitoring Department 302 is notified of the instruction of the location which a program counter points out next, i.e., the instruction which it is going to execute next, from the program interpretation activation section 301 which is interpreting the executive program 101 serially, and the function ID corresponding to the instruction obtains, and it outputs a function ID by performing monitor processing later mentioned with reference to the function ID table 310.

[0025] The function ID outputted from the use functional Monitoring Department 302 and execution-time use functional information 102 carry out as an input, and the execution-time use functional monitor Banking Inspection Department 303 tells interpretation activation of an executive program 101 to the program interpretation activation section 301 as stopping, when the function ID matched with the flag of the purport do not use it in the execution-time use functional information 102 is outputted from the use functional Monitoring Department 302.

[0026] The disable table 304 is a table which recorded the information which shows [which it has permitted using the function to the executive program 101 of the downloaded object program 100 about each of all functions that may be used for the application program which operates on program execution equipment 300 / or or] whether prohibition is carried out.

[0027] Drawing 5 is drawing showing the DS and the example of contents of the disable table 304. As shown in this drawing, a disable table is a table which consists of a set of a group with the flag 602 which shows [to which use of the function shown by the function ID 601 and its function ID is permitted / or or] whether prohibition is carried out. A function ID 601 assigns an identifier so that the function which may be used for an application program may be

classified and it may become each classified function with a meaning, the function corresponding to the library called from an application program is included in each of that function, and the function corresponding to a load instruction or store instruction is further included in it. That is, the function ID included in a function ID table or execution-time use functional information was altogether included on the disable table upwards, and the function ID corresponding to a load instruction or store instruction is included in it.

[0028] A flag 602 shows the purport which 0x00 forbids use, and shows the purport which 0x01 permits use. In the example of contents shown in this drawing, for example as a thing corresponding to a load instruction The function of the function ID of 0x0101 which means data read-out from an individual humanity news field, The function of the function ID of 0x0102 which means data read-out from a system area, As a thing corresponding to store instruction, the function of the function ID of 0x0201 which means the data store to an individual humanity news field, and the function of the function ID of 0x0202 which means the data store to a system area show that use is forbidden. In addition, an individual humanity news field and a system area are explained later.

[0029] The execution-time use functional prohibition Banking Inspection Department 305 moreover, by comparing these with reference to the execution-time use functional information 102 and the disable table 304 When the same function ID as the function ID matched with the flag of the purport used in the execution-time use functional information 102 is matched with the flag of the purport which forbids use in the disable table 304 It is told to the program interpretation activation section 301 that interpretation activation of an executive program 101 is suspended.

[0030] The monitor prohibition Banking Inspection Department 306 considers the function ID outputted from the use functional Monitoring Department 302, and the disable table 304 as an input, and when the function ID matched with the flag of the purport which forbids use in a disable table is outputted from the use functional Monitoring Department 302, interpretation activation of an executive program 101 is told to the program interpretation activation section 301 as stopping.

[0031] The user notification section 307 is controlled to display the purport which interpretation activation of the executive program 101 by the program interpretation activation section 301 stopped on the display of a portable telephone, and notifies a program execution halt to a user. The program execution authorization judging section 308 is what constitutes the user interface at the time of a halt of interpretation activation with the user notification section 307. When it controls so that the user notification section 307 displays the purport of a halt of interpretation activation of an executive program 101 on a display Assignment by the user of whether a halt of an executive program 101 is canceled or to end activation of an executive program 101 is received through the various carbon buttons of a portable telephone etc., and discharge of a halt or directions of termination is told to the program interpretation activation section 301 according to the assignment.

[0032] The user prohibition assignment input section 309 receives the input about modification of the contents of the disable table 304 from a user through the various carbon buttons of a portable telephone etc., and updates the disable table 304 according to the input. When the user prohibition assignment input section 309 exists, a user can specify [which it permits that a specific function is used by the downloaded application program / or or] whether prohibition is carried out.

[0033] Moreover, the function ID table 310 is a table of the same contents as the function ID table 201, and is a table which has the structure shown in drawing 3 . In addition, program execution equipment 300 has the function stored in the memory with which minded the base transceiver station, acquired namely, downloaded the application program by communication link, and the portable telephone was equipped.

[0034] Drawing 2 is drawing showing the relation between the portable telephone 320 equipped with program execution equipment 300, and the object program for download. The object program 100 offered from the program generator equipped with program generation equipment 200 for the purpose of downloading to a portable telephone is stored in the program storing server 250 which is the computer connected to the public network. The portable telephone 320 equipped with program execution equipment 300 can download the object program 100 stored in the program storing server 250 through the base transceiver station 260 by radiocommunicating with a base transceiver station 260.

[0035] <Memory structure> Here, the memory which the application program which program execution equipment 300 performs can access is explained. Memory is divided into the individual humanity news field for recording individual humanity news, the system area for recording an operating system and information required for activation of an interpreter function, and other fields.

[0036] Drawing 6 is drawing having shown the classification of the field in memory. As shown in this drawing, from the 0x0000th street to a 0x3FFF address is a system area, from the 0x4000th street to a 0x7FFF address is an individual humanity news field, and memory is other fields from the 0x8000th street to whose 0xFFFF addresses are not a system area or an individual humanity news field, either.

[0037] That is, with the application program built in the portable telephone from the beginning, individual humanity news is recorded on an individual humanity news field, and program execution equipment 300 accesses a system area, and performs record and read-out of data required for activation of processing. Drawing 7 is drawing showing the example of the contents of individual humanity news. As shown in this drawing, individual humanity news includes the information in connection with the privacy of individuals, such as a person name and the telephone number. Therefore, the individual humanity news stored in this individual humanity news field should be protected especially from unjust access.

Actuation of program execution equipment 300 equipped with an above-mentioned configuration is explained below <actuation>.

[0038] <Interpretation activation actuation> drawing 8 is a flow chart which shows the procedure at the time of carrying out interpretation activation of the object program which program execution equipment 300 downloaded. After program execution equipment 300 downloads an object program 100 by the communication link with a base transceiver station and stores it in memory, it begins interpretation activation.

[0039] It faces that the program interpretation activation section 301 performs interpretation activation of an executive program 101. First the execution-time use functional prohibition Banking Inspection Department 305 The execution-time use functional information 102 is accessed by referring to the attribute information identified with the specific identification number of a Java class file. The execution-time use functional information 102 is compared with the disable table 304 (step S101). Either judges whether it is in agreement with the function ID matched with the flag of a purport with which use is forbidden in the disable table among the functions ID matched with the flag of the purport used in the execution-time use functional information 102 (step S102).

[0040] When it judges with it being in agreement in step S102, the execution-time use functional prohibition Banking Inspection Department 305 notifies a halt to the program interpretation activation section 301 and the user notification section 307, when it judges with program execution equipment 300 performing interpretation activation halt processing (step S103), and not being in agreement, step S103 is skipped, and monitor processing is carried out continuously (step S104). In addition, interpretation activation halt processing is explained later.

[0041] Here, monitor processing is explained. Drawing 9 is a flow chart which shows the monitor processing by the use functional Monitoring Department 302. The program interpretation activation section 301 obtains the instruction executed next with reference to a program counter, and transmits it to the use functional Monitoring Department 302 (step S201). The use functional Monitoring Department 302 judges whether the instruction is a data read-out instruction of aload etc. (step S202), and if it is a data read-out instruction, based on the operand of the instruction, the read-out address which is the location set as the read-out object in memory will be acquired (step S203). Even if it is the case where the read-out address is specified with the register etc., the actual read-out address is acquired by referring to contents values, such as the register in the case of activation of step S203.

[0042] After acquiring the read-out address, if the read-out address judges whether it is what points out the inside of a system area (step S204) and the inside of a system area is pointed out, it will tell the execution-time use functional monitor Banking Inspection Department 303 and the monitor prohibition Banking Inspection Department 306 the function ID of 0x0102, and will end monitor processing (step S205). If it judges whether the read-out address will be what points out the inside of an individual humanity news field if the inside of a system area is not pointed out in step S204 (step S206) and the inside of an individual humanity news field is pointed out, the function ID of 0x0101 will be told to the execution-time use functional

monitor Banking Inspection Department 303 and the monitor prohibition Banking Inspection Department 306, and monitor processing will be ended (step S207).

[0043] If the inside of an individual humanity news field is not pointed out in step S206, the function ID of 0x0000 will be told to the execution-time use functional monitor Banking Inspection Department 303 and the monitor prohibition Banking Inspection Department 306, and monitor processing will be ended (step S208). When the obtained instruction is not a data read-out instruction, (step S202) and the use functional Monitoring Department 302 judge whether the instruction is a data write-in instruction of astore etc. (step S209), and if it is a data write-in instruction, based on the operand of the instruction, the write address which is the location set as the write-in object in memory will be acquired (step S210). Even if it is the case where the write address is specified with the register etc., an actual write address is acquired by referring to contents values, such as the register in the case of activation of step S210.

[0044] After acquiring a write address, if the write address judges whether it is what points out the inside of a system area (step S211) and the inside of a system area is pointed out, it will tell the execution-time use functional monitor Banking Inspection Department 303 and the monitor prohibition Banking Inspection Department 306 the function ID of 0x0202, and will end monitor processing (step S212). If it judges whether a write address will be what points out the inside of an individual humanity news field if the inside of a system area is not pointed out in step S211 (step S213) and the inside of an individual humanity news field is pointed out, the function ID of 0x0201 will be told to the execution-time use functional monitor Banking Inspection Department 303 and the monitor prohibition Banking Inspection Department 306, and monitor processing will be ended (step S214).

[0045] If the inside of an individual humanity news field is not pointed out in step S213, the function ID of 0x0000 will be told to the execution-time use functional monitor Banking Inspection Department 303 and the monitor prohibition Banking Inspection Department 306, and monitor processing will be ended (step S215). For (step S209) and the use functional Monitoring Department 302, the instruction is invoke when the obtained instruction is not a data write-in instruction. It judges whether it is the library call instruction of virtual etc. (step S216). If it is a library call instruction, will obtain a library number from the operand of the instruction, and the function ID corresponding to the library number will be acquired by referring to the function ID table 310. The function ID is told to the execution-time use functional monitor Banking Inspection Department 303 and the monitor prohibition Banking Inspection Department 306, and monitor processing is ended (step S217).

[0046] Moreover, if it is not a library call instruction in step S216, the use functional Monitoring Department 302 will tell the execution-time use functional monitor Banking Inspection Department 303 and the monitor prohibition Banking Inspection Department 306 the function ID of 0x0000, and will end monitor processing (step S218). In addition, the function ID outputted from the use functional Monitoring Department 302 can identify now

the function ID corresponding to a library call instruction, and the function ID corresponding to the other instruction, and that 8 bits of whose high orders are 0x00 among Functions ID is presupposing that it is it a thing corresponding to a library call instruction here.

[0047] Hereafter, it returns to explanation adapted to drawing 8 . The function ID in which the execution-time use functional monitor Banking Inspection Department 303 was outputted from the use functional Monitoring Department 302 as a result of monitor processing after the monitor processing (step S104) mentioned above A compare check with the execution-time use functional information 102 is conducted (step S105). The same function ID as the function ID outputted as a result of the function ID of the function used with the instruction executed after in an executive program 101, i.e., monitor processing, sets to the execution-time use functional information 102. It judges whether it is matched with the flag of the purport which is not used (step S106). Step S106 has the semantics of judging whether it having used the function it is declared that does not use it using the execution-time use functional information 102 on the occasion of actual activation.

[0048] It restricts, when it is the function ID matched with the flag of the purport which the function ID outputted as a result of monitor processing in step S106 does not use in the execution-time use functional information 102. The execution-time use functional monitor Banking Inspection Department 303 notifies a halt to the program interpretation activation section 301 and the user notification section 307, and program execution equipment 300 performs interpretation activation halt processing (step S107). In the case of others, step S107 is skipped, and the monitor prohibition Banking Inspection Department 306 conducts the compare check of the function ID outputted as a result of monitor processing after that, and a disable table (step S108).

[0049] In step S108, the monitor prohibition Banking Inspection Department 306 judges whether the same function ID as the function ID outputted as a result of monitor processing is matched with the flag of the purport which forbids use in a disable table (step S109). It restricts, and when the function ID outputted as a result of monitor processing is the function ID matched with the flag of the purport which forbids use in a disable table, a halt is notified to the program interpretation activation section 301 and the user notification section 307, interpretation activation halt processing carries out (step S110), and, in the case of others, the monitor prohibition Banking Inspection Department 306 skips step S110 as a result of this judgment.

[0050] Then, the program interpretation activation section 301 carries out interpretation activation of the instruction which should be executed, the instruction, i.e., the degree, set as the object of monitor processing, (step S111). After processing of S111 is repeated from step S104 and interpretation activation of all processings is completed until interpretation activation of all processings of the executive program 101 by the program interpretation activation section 301 is completed, actuation of program execution equipment is also ended (step S112).

[0051] Hereafter, interpretation activation halt processing is explained. Drawing 10 is a flow chart which shows interpretation activation halt processing. The program interpretation activation section 301 which received the notice of a halt sets up the control state by an internal variable etc. so that interpretation activation of an executive program may be suspended (step S301), and the user notification section 307 notifies to a user that interpretation activation was suspended (step S302).

[0052] The screen displayed on a display by control of the user notification section 307 in this step S302 is shown in drawing 11 . This screen tells the carbon button used when directing continuation of activation to a user, while the purport by which activation of the executive program 101 whose file name is maze.cj was suspended is shown.

[0053] After issuing [of a halt] a memorandum to the user by the user notification section 307, the program execution authorization judging section 308 receives and interprets a user's input (step S303), and it judges whether it is the input of directions of the purport which continues interpretation activation of an executive program 101 (step S304). When it judges as directions of continuation of interpretation activation in step S304, the program execution authorization judging section 308 directs discharge of a halt of interpretation activation in the program interpretation activation section 301, and in response, the program interpretation activation section 301 sets up a control state so that a halt of interpretation activation may be canceled (step S305). An executive program 101 carries out interpretation activation succeedingly by this step S305.

[0054] Moreover, when it is judged that they are not directions of continuation of interpretation activation in step S304, termination of interpretation activation in the program interpretation activation section 301 is directed, and in response, the program execution authorization judging section 308 sets up a control state in the program interpretation activation section 301 so that interpretation activation may be ended. (Step S306) . It is lost that interpretation activation of the executive program 101 is henceforth carried out by this step S306, and actuation of program execution equipment 300 is ended.

[0055] <Renewal actuation of disable table> program execution equipment 300 has the function which updates a disable table during interpretation activation of a program at the time of except. If this function is performed corresponding to predetermined actuation when the specific carbon button of a portable telephone is pushed by the user and predetermined actuation is performed, the user prohibition assignment input section 309 will be controlled to display the disable function selection screen as shown in the display of a portable telephone at drawing 12 , and will receive the input about assignment of the disable function by the user.

[0056] The user prohibition assignment input section 309 displays a functional item etc., as shown in drawing 12 , the display of a functional item is scrolled according to a user's specific button grabbing, and the disable table 304 is updated so that use of the function to express with the functional item by which highlighting is carried out to receiving the carbon button input of "1" or "0" may be carried out as authorization or prohibition.

[0057] Thereby, a user can define now the function to forbid use. For example, if it is the user who considers that it may be read by individual humanity news, it will become possible to change the disable table 304 so that use of the function of data read-out from an individual humanity news field may be permitted.

Although the program execution equipment concerning this invention was explained using the gestalt of operation more than the <supplement>, this invention is not restricted to what was shown in the gestalt of operation. Namely, with the gestalt of (1) book operation, although the address shall be defined fixed, the field in the memory in which individual humanity news is stored etc. It supposes that a flag is added for every data of specific size, and becomes possible [enabling it to identify whether it is individual humanity news or they are the information on other with the flag, then also distributing and storing individual humanity news in the address of the arbitration in room]. That is, it is good also as two or more individual humanity news fields of the specific size which is not fixed existing.

[0058] Drawing 13 is drawing showing the example stored so that the data which are individual humanity news, and the data which are except individual humanity news may become identifiable with a flag in memory. A flag takes the value of 0 or 1, and this drawing shows that it is individual humanity news, if a flag is 1. In such a case, suppose that the flag added to the data with which the address points [the read-out address or the write address in monitor processing] out decision (steps S206 and S213) of being the inside of an individual humanity news field carries out based on 0 or 1. In addition, it is good also as adding a flag which identifies individual humanity news, system data, and other data for every data of specific size, then making a judgment (steps S204 and S211) of being the inside of a system area by the same approach.

(2) The partition of the function shown in the disable table 304 or the execution-time use functional information 102 grade in the gestalt of this operation may be a mere example, and may be other partitions. Moreover, although a function ID table is the table which enumerated the functions corresponding to a library call instruction and it is the information which matched with execution-time use functional information 102 the flag of whether it is used about all the functions that may be performed with a library call instruction, or not to carry out, it is good also as incorporating the information about the function performed with other specific instructions which are not library call instructions. However, it is desirable for the check of the existence of use of the function to be able to perform simply the function in which Function ID is included in a function ID table and execution-time use functional information, before program execution.

[0059] In addition, since the function which can use when an object program calls the library usually prepared for the device side by which program execution equipment was carried is the function of using the specific resource of the device, if a function ID table is the table which enumerated the functions of corresponding for every library, in order to attain the purpose of security reservation of avoiding an object program performing risk actuation, it can say

becoming with what is suitable.

(3) Although the gestalt of this operation showed the example which forbids the data output to a wireless interface, and the data input from a wireless interface on a disable table (refer to drawing 5), it is good also as not necessarily having to forbid these and forbidding the data I/O to other circuits, and the function realized by other library calls may be forbidden. Moreover, it is good also as forbidding the call origination function to the exterior, i.e., the function to telephone, instead of forbidding the function of the data input from a wireless interface, and the data output to a wireless interface.

[0060] In addition, it is useful practically to forbid the data I/O which leads a wireless interface in the semantics which prevents communicating with the exterior, before a user knows. Moreover, it may be useful in the field of prevention of unjust information acquisition of tapping etc., and prevention of a troublesome output to forbid the data output to the output device in large semantics, such as to forbid the data acquisition from the input device in large semantics, such as a carbon button, a switch, a dial, a mouse, a trackball, a joy stick, a keyboard, a microphone, a camera, and a sensor, for example, and a display, LED, a lamp, a loudspeaker, vibrator.

[0061] Moreover, although the gestalt of this operation showed the example which forbids the data store to data read-out from an individual humanity news field, data read-out from a system area, and an individual humanity news field, and the data store to a system area on a disable table, these must not necessarily be forbidden and you may make it forbid activation of other specific instructions. In addition, it is useful practically from fields, such as privacy protection, to forbid access to individual humanity news.

(4) A user's input shown at step S303 of drawing 10 in the gestalt of this operation is good also as being made not only through a carbon button but through other input devices. Moreover, in step S303, what a user did not operate may be carried out to interpreting it as what inputted specific assignment according to the agreement defined beforehand. For example, if nothing is inputted for 30 seconds after the purport which the executive program stopped is displayed on a display, the program execution authorization judging section 308 is good also as interpreting it as assignment that interpretation activation of the executive program was not continued having been made by the user.

(5) In case a portable telephone downloads the object program 100 shown in drawing 2 in the gestalt of this operation, in order to check the justification of the program storing server 250 which is the distribution side of the object program 100, it is good also as performing mutual recognition etc.

[0062] Moreover, it is good also as being what is not limited to this and applied to other household-electric-appliances devices and Personal Digital Assistants although a portable telephone shall be equipped with program execution equipment 300 with the gestalt of this operation. Moreover, it is good also as an object program being transmitted by approach which is not limited to what also showed the acquisition path of the object program set as the

activation object of program execution equipment 300 to drawing 2 , for example, is set to Bluetooth, HomeRF, etc.

(6) Although [the application program to download, i.e., an object program, / the gestalt of this operation] it is a Java class file, it is not limited to this and is good also as being a machine program. In the case of a machine program, the program interpretation activation section 301 decides to be CPU, and the use functional Monitoring Department 302 is good also as supervising the instruction executed next with reference to each register and memory, whenever the register equivalent to the so-called program counter changes.

(7) Although step S306 of drawing 10 shown with the gestalt of this operation only ends interpretation activation of an executive program, its step S306 is good also as deleting the ended executive program and the execution-time use functional information which accompanies this from the inside of the storage of a portable telephone further. Moreover, when program execution equipment 300 performs the downloaded object program and it progresses to branching of YES at step S112 of drawing 8 , it is good also as adding the next processing. The processing is processing for making the object program which activation completed applicable [, such as the usual interpreter,] to activation after next time, for example, can consider the processing which registers the file name of the object program into the list of safe application programs, the processing which records the information on a purport safe for the attribute information on a Java class file. In addition, I hear that semantics of saying [that an object program is set as the activation objects, such as the usual interpreter,] is performed without performing processing for inhibiting activation of unjust functions, such as a use functional monitor, and there is. About the program safeties, such as an object program which follows, for example, is registered into the list of safe application programs, and an object program with which the information on a safe purport was added, were guaranteed to be, it is good also as performing the program only using the same function as the conventional interpreter, without program execution equipment 300 inhibiting activation of an unjust function.

(8) After the program generation equipment 200 shown with the gestalt of this operation generated an object program, although [equipment] the function ID of the function which the object program uses searches and execution-time use functional information generates, the function which will carry out object program use may grasp, and it may generate execution-time use functional information in the process which translates to an object program in the source program described in C, Java language, etc.

[0063] Moreover, program generation equipment 200 is good also as enciphering in order to protect the execution-time use functional information included in an object program from the alteration in a distribution path. In this case, execution-time use functional information is decoded and it is necessary to make it refer to in the program execution equipment 300 side.

With the gestalt of this operation, (9) In an individual humanity news field As the individual humanity news of a person name, the telephone number, and a mail address and others being

contained Deciding [and] to forbid use of the data store to the individual humanity news field by the downloaded object program, or the function of data read-out from an individual humanity news field, the user decided that use of these functions can be changed into authorization from prohibition by renewal of a disable table. Thus, it is good also as not managing individual humanity news all together, but classifying individual humanity news into two or more classification, and managing it for every classification. That is, it is good also as classifying an individual humanity news field with the 1st sort individual humanity news field, the 2nd sort individual humanity news field, the 3rd sort individual humanity news field, etc., and performing data store by this classified object program that downloaded for every field, and prohibition of read-out or control of authorization.

(10) The vocabulary "a halt" used about interpretation activation of an executive program in the gestalt of this operation means "suppression" of interpretation activation, when performing processing shown in steps S101 and S102 of drawing 8 before starting of an executive program. In addition, though program execution equipment 300 loads each module to memory dynamically and performs it at the time of the need, when an executive program consists of two or more modules, since it is good and it good also as processing steps S101-S103 immediately after loading in this case, it does not necessarily restrict inhibiting interpretation activation before starting of an executive program, but the case which suspends interpretation activation during activation of an executive program may also happen.

(11) It is good for the screen shown in drawing 11 in the gestalt of this operation also as adding useful information to decision by the user of whether to make a halt cancel -- whether it was stopped in order that an executive program might use which function.

(12) The computer program for making a household-electric-appliances device, a Personal Digital Assistant, etc. which have a program execution function perform procedure (procedure shown in drawing 8 - drawing 10) of the program execution equipment 300 in the gestalt of this operation can be recorded on a record medium, or can be circulated through various channels etc., and can also be distributed. There are an IC card, an optical disk, a flexible disk, a ROM, etc. in such a record medium. Use is presented with the computer program circulated and distributed by carrying out install etc. to a household-electric-appliances device, a Personal Digital Assistant, etc., and a household-electric-appliances device, a Personal Digital Assistant, etc. realize program execution equipment as performed said computer program and shown with the gestalt of this operation.

[0064]

[Effect of the Invention] The program execution control unit concerning this invention so that clearly from the above explanation It is carried in the device and the program to which the use functional information which shows the function which oneself uses among the functional groups using the specific resource of said device was added is acquired. An acquisition means to be the program execution control unit to perform and to acquire a program from a channel,

It is characterized by having the means for stopping which stops the program execution by said activation means in the predetermined case which makes a judgment based on said use functional information, and expresses that the decision result of program execution is unsuitable as an activation means to perform the acquired program.

[0065] Since the use functional information that this shows beforehand the function which that program uses for a program is added, it becomes possible by using this use functional information to secure security by the comparatively simple approach. Namely, it can realize [whether the program uses the function in which use should be forbidden, and] now by the configuration with simple detecting detecting that the program is altered and by referring to use functional information by comparing use functional information with actuation of an actual program.

[0066] Said program is that to which said activation means executes the instruction in said program including two or more instructions. Moreover, said means for stopping When it is the instruction which uses the function which is not shown as a function which supervises the instruction used as the candidate for activation to the degree in the program under activation, and said instruction uses for it in said use functional information among said functional groups, it is good also as stopping said program execution by said activation means.

[0067] Since the use functional information which shows the function which it is added by this to the downloaded program, and the program uses will be compared with the result of having supervised the function which the program tends to use at the time of actual actuation, it is detectable in the difference with use functional information and a program. Therefore, if premised on use functional information and a program being what is adjusted in a program generate time, that the program is unjustly altered in a channel can detect easily, and it can prevent the damage by the program execution altered unjustly.

[0068] Moreover, said use functional information is enciphered and said means for stopping is good also as decoding and referring to said use functional information. Thereby, since use functional information is enciphered, the alteration of a program becomes detectable easily by it becoming difficult to rewrite both a program's and use functional information's unjustly in a communication path, consequently investigating the mismatching of a program and use functional information.

[0069] Moreover, said program execution control unit has a prohibition functional storage means memorize the prohibition functional information which shows the function forbid use, and when the function forbid the use shown in said prohibition functional information is shown as a function use it to said use functional information, it is good also as stopping the program execution by said activation means in said means for stopping.

[0070] Since the program execution it is indicated to be to use the function which this has determined as what forbids use beforehand from the reasons of risk etc. is stopped, safety is securable by the simple approach of only a comparison of use functional information and prohibition functional information. In addition, the suppression which does not perform the

program execution itself is also included in a halt here. Moreover, it is good for the function to forbid the use which said prohibition functional information shows, also as the function of radio being included at least.

[0071] Thereby, there is possibility of an outflow of extra sensitive information, and making it use it freely [the reasons nil why a communication link tariff may be needed] to the downloaded program can stop the program which uses a radio function with a problem. Moreover, it is good for the function to forbid the use which said prohibition functional information shows, also as the function of the data output from an output device being included at least.

[0072] It can prevent performing output actuation of the downloaded program displaying secret information, such as a password, on a display by this. Moreover, it is good for the function to forbid the use which said prohibition functional information shows, also as the function of the data acquisition from an input device being included at least. It can prevent performing data acquisition actuation of the downloaded program intercepting by acquiring data through a microphone by this.

[0073] Moreover, said program execution control unit is good also as having a prohibition functional modification means to receive actuation of a user and to update said prohibition functional information further according to said actuation. a user can set up now freely a function [responds to the ability of some users not to also consider the function which this has determined as what forbids use beforehand from the reasons of risk etc. to be risk, and] to make it use for the downloaded program.

[0074] Moreover, the program execution control unit concerning this invention An acquisition means to be the program execution control unit which acquires and performs the program which is carried in a Personal Digital Assistant equipped with the memory which has an individual humanity news field, and consists of two or more instructions, and to acquire a program from a channel, An activation means to perform the acquired program, and the program under activation supervise the instruction which it is going to execute next. When said instruction is an instruction which performs data read-out from said individual humanity news field, it is characterized by having the means for stopping which stops said program execution by said activation means.

[0075] Since it can prevent the program which is usually memorized by the Personal Digital Assistant and downloaded by this the individual humanity news which is the information in connection with privacy reading, the outflow of individual humanity news can be prevented. Moreover, the program execution control unit concerning this invention An acquisition means to be the program execution control unit which acquires and performs the program which is carried in a Personal Digital Assistant equipped with the memory which has an individual humanity news field, and consists of two or more instructions, and to acquire a program from a channel, An activation means to perform the acquired program, and the program under activation supervise the instruction which it is going to execute next. When said instruction is

an instruction which performs the data store to said individual humanity news field, it is characterized by having the means for stopping which stops said program execution by said activation means.

[0076] It can prevent now the program which is usually memorized by the Personal Digital Assistant and downloaded by this the individual humanity news which is the information in connection with privacy rewriting. Moreover, the program execution control unit concerning this invention An acquisition means to be the program execution control unit which acquires and performs the program which is carried in a Personal Digital Assistant and consists of two or more instructions, and to acquire a program from a channel, An activation means to perform the acquired program, and the program under activation supervise the instruction which it is going to execute next. When it is the instruction which calls the functional manipulation routine to which said instruction is the functional manipulation routine with which said Personal Digital Assistant is equipped, and communicates with the exterior of said Personal Digital Assistant, it is characterized by having the means for stopping which stops said program execution by said activation means.

[0077] Here, a functional manipulation routine is the so-called subroutine which exists in the execution environment of an application program, is called from the application program, and performs a certain processing, for example, is invoke. It is the library program called with the library call instruction of virtual etc. It can prevent now using the function in which the downloaded program communicates with the exterior of a Personal Digital Assistant by this. This is useful at a point with semantics, such as preventing the situation where a communication link tariff is needed regardless of an intention of a user arising.

[0078] Moreover, said functional manipulation routine is good also as being the functional manipulation routine which performs data transmission to the exterior of said Personal Digital Assistant. Thereby, the outflow of the extra sensitive information from a Personal Digital Assistant can be prevented now. Moreover, the program execution control unit concerning this invention An acquisition means to be the program execution control unit which acquires and performs the program which is carried in a Personal Digital Assistant and consists of two or more instructions, and to acquire a program from a channel, An activation means to perform the acquired program, and the program under activation supervise the instruction which it is going to execute next. The means for stopping which stops said program execution by said activation means when said instruction is the functional manipulation routine with which said Personal Digital Assistant is equipped and it is the instruction which calls the functional manipulation routine which performs data output from the output device with which said Personal Digital Assistant is equipped It is characterized by having.

[0079] It can prevent performing output actuation of the downloaded program displaying secret information, such as a password, on the display of a Personal Digital Assistant by this. Moreover, the program execution control unit concerning this invention An acquisition means

to be the program execution control unit which acquires and performs the program which is carried in a Personal Digital Assistant and consists of two or more instructions, and to acquire a program from a channel, An activation means to perform the acquired program, and the program under activation supervise the instruction which it is going to execute next. The means for stopping which stops said program execution by said activation means when said instruction is the functional manipulation routine with which said Personal Digital Assistant is equipped and it is the instruction which calls the functional manipulation routine which performs data acquisition from the input device with which said Personal Digital Assistant is equipped It is characterized by having.

[0080] It can prevent performing data acquisition actuation of the downloaded program intercepting by this by acquiring data through the microphone with which the Personal Digital Assistant was equipped. Moreover, said program execution control unit is still better also as having a notice means to notify a user of the stopped purport, when said program execution stops by said means for stopping.

[0081] Thereby, a user can know now that the downloaded program execution was stopped. Moreover, said program execution control unit is still better also as having a halt discharge means to receive the input by the user and to cancel a halt according to said input, when said program execution stops by said means for stopping.

[0082] Thereby, a user can cancel [self decision] the halt, when program execution is stopped.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram of the program execution equipment 300 grade concerning the gestalt of operation of this invention.

[Drawing 2] It is drawing showing the relation between a portable telephone equipped with program execution equipment 300, and the object program for download.

[Drawing 3] It is drawing showing the DS and the example of contents of a function ID table.

[Drawing 4] It is drawing showing the DS and the example of contents of execution-time use functional information which are added to an object program.

[Drawing 5] It is drawing showing the DS and the example of contents of the disable table 304.

[Drawing 6] It is drawing having shown the classification of the field in memory.

[Drawing 7] It is drawing showing the example of the contents of individual humanity news.

[Drawing 8] It is the flow chart which shows the procedure at the time of carrying out interpretation activation of the object program which program execution equipment 300 downloaded.

[Drawing 9] It is the flow chart which shows the monitor processing by the use functional Monitoring Department 302.

[Drawing 10] It is the flow chart which shows interpretation activation halt processing.

[Drawing 11] It is drawing showing the example of the screen displayed on a display by control of the user notification section 307.

[Drawing 12] It is drawing showing the disable function selection screen controlled so that the user prohibition assignment input section 309 displays on the display of a portable telephone.

[Drawing 13] It is drawing showing the example stored so that the data which are individual humanity news, and the data which are except individual humanity news may become identifiable with a flag in memory.

[Description of Notations]

100 Object Program

101 Executive Program

102 Execution-Time Use Functional Information

200 Program Generation Equipment

201 Function ID Table

202 Execution-Time Use Functional Information Generation Section

300 Program Interpretation Activation Equipment

300 Program Execution Equipment

301 Program Interpretation Activation Section

302 Use Functional Monitoring Department

303 Execution-Time Use Functional Monitor Banking Inspection Department

304 Disable Table

305 Execution-Time Use Functional Prohibition Banking Inspection Department

306 Monitor Prohibition Banking Inspection Department

307 User Notification Section

308 Program Execution Authorization Judging Section

309 User Prohibition Assignment Input Section

310 Function ID Table

---

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－41170
（P2002－41170A）
(43)公開日　平成14年２月８日(2002.2.8)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード'（参考）
Ｇ０６Ｆ　1/00		Ｇ０６Ｆ　12/14	３１０Ｚ　５Ｂ０１７
12/14	３１０	9/06	６６０Ｊ　５Ｂ０７６

審査請求　未請求　請求項の数17　ＯＬ　（全 16 頁）

(21)出願番号　特願2000－227840(P2000－227840)

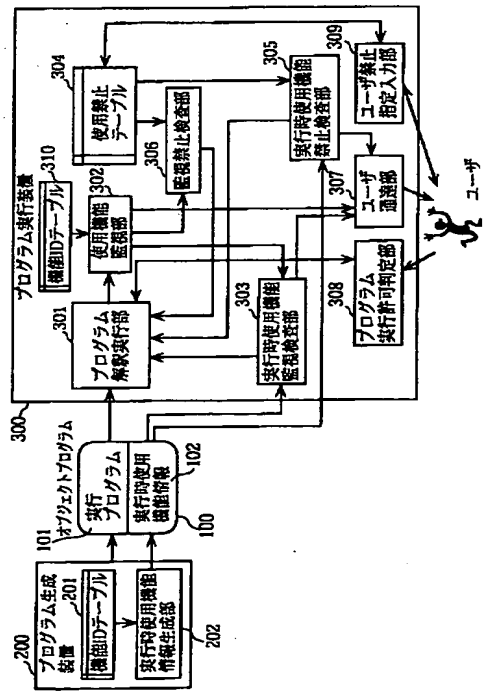
(22)出願日　平成12年７月27日(2000.7.27)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　金丸　智一
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　和氣　裕之
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100090446
弁理士　中島　司朗　（外１名）

最終頁に続く

(54)【発明の名称】　プログラム実行制御装置

(57)【要約】
【課題】　ダウンロードしたプログラムの実行に際してのセキュリティ確保を簡易に行う手段を提供する。
【解決手段】　携帯電話機に搭載されたプログラム実行装置３００は、使用する機能を宣言した実行時使用機能情報１０２が付加された実行プログラム１０１を通信路より取得して、プログラム解釈実行部３０１によって逐次実行する。実行プログラム１０１の実行に際して、プログラム実行装置３００は、使用を禁止する機能を示す使用禁止テーブル３０４に含まれる機能が実行時使用機能情報１０２において使用宣言されていると実行を停止する。また実行プログラム１０１の実行中に次に実行する命令を監視することにより、その命令により利用される機能が実行時使用機能情報１０２で使用宣言されていないものであれば実行を停止する。



1

【特許請求の範囲】

【請求項１】　機器に搭載されており、前記機器の特定の資源を利用する機能群のうち自らが使用する機能を示す使用機能情報が付加されたプログラムを取得して、実行するプログラム実行制御装置であって、
通信路からプログラムを取得する取得手段と、
取得したプログラムを実行する実行手段と、
前記使用機能情報に基づく判断を行い、判断結果がプログラムの実行が不適当であることを表す所定の場合に、前記実行手段によるプログラムの実行を停止させる停止手段とを備えることを特徴とするプログラム実行制御装置。

【請求項２】　前記プログラムは複数の命令を含み、
前記実行手段は前記プログラム中の命令を実行するものであり、
前記停止手段は、実行中のプログラムにおける次に実行対象となる命令を監視し、前記命令が前記機能群のうち前記使用機能情報において使用する機能として示されていない機能を使用する命令であった場合に前記実行手段による前記プログラムの実行を停止させることを特徴とする請求項１記載のプログラム実行制御装置。

【請求項３】　前記使用機能情報は暗号化されており、
前記停止手段は前記使用機能情報を復号して参照することを特徴とする請求項２記載のプログラム実行制御装置。

【請求項４】　前記プログラム実行制御装置は、使用を禁止する機能を示す禁止機能情報を記憶する禁止機能記憶手段を備え、
前記停止手段は、前記禁止機能情報に示されている使用を禁止する機能が前記使用機能情報に使用する機能として示されている場合には前記実行手段によるプログラムの実行を停止させることを特徴とする請求項１記載のプログラム実行制御装置。

【請求項５】　前記禁止機能情報が示す使用を禁止する機能には、少なくとも無線通信の機能が含まれることを特徴とする請求項４記載のプログラム実行制御装置。

【請求項６】　前記禁止機能情報が示す使用を禁止する機能には、少なくとも出力デバイスからのデータ出力の機能が含まれることを特徴とする請求項４記載のプログラム実行制御装置。

【請求項７】　前記禁止機能情報が示す使用を禁止する機能には、少なくとも入力デバイスからのデータ取得の機能が含まれることを特徴とする請求項４記載のプログラム実行制御装置。

【請求項８】　前記プログラム実行制御装置はさらに、ユーザの操作を受け付けて前記操作に応じて前記禁止機能情報を更新する禁止機能変更手段を備えることを特徴とする請求項４～７のいずれか１項に記載のプログラム実行制御装置。

【請求項９】　個人情報領域を有するメモリを備える携帯情報端末に搭載され、複数の命令からなるプログラムを取得して実行するプログラム実行制御装置であって、
通信路からプログラムを取得する取得手段と、
取得したプログラムを実行する実行手段と、
実行中のプログラムが次に実行しようとする命令を監視し、前記命令が前記個人情報領域からのデータ読出を行う命令である場合に前記実行手段による前記プログラムの実行を停止させる停止手段とを備えることを特徴とするプログラム実行制御装置。

【請求項１０】　個人情報領域を有するメモリを備える携帯情報端末に搭載され、複数の命令からなるプログラムを取得して実行するプログラム実行制御装置であって、
通信路からプログラムを取得する取得手段と、
取得したプログラムを実行する実行手段と、
実行中のプログラムが次に実行しようとする命令を監視し、前記命令が前記個人情報領域へのデータ書込を行う命令である場合に前記実行手段による前記プログラムの実行を停止させる停止手段とを備えることを特徴とするプログラム実行制御装置。

【請求項１１】　携帯情報端末に搭載され、複数の命令からなるプログラムを取得して実行するプログラム実行制御装置であって、
通信路からプログラムを取得する取得手段と、
取得したプログラムを実行する実行手段と、
実行中のプログラムが次に実行しようとする命令を監視し、前記命令が前記携帯情報端末が備える機能処理ルーチンであって前記携帯情報端末の外部と通信する機能処理ルーチンを呼び出す命令である場合に前記実行手段による前記プログラムの実行を停止させる停止手段とを備えることを特徴とするプログラム実行制御装置。

【請求項１２】　前記機能処理ルーチンは前記携帯情報端末の外部へのデータ送信を行う機能処理ルーチンであることを特徴とする請求項１１記載のプログラム実行制御装置。

【請求項１３】　携帯情報端末に搭載され、複数の命令からなるプログラムを取得して実行するプログラム実行制御装置であって、
通信路からプログラムを取得する取得手段と、
取得したプログラムを実行する実行手段と、
実行中のプログラムが次に実行しようとする命令を監視し、前記命令が前記携帯情報端末が備える機能処理ルーチンであって前記携帯情報端末が備える出力デバイスからのデータ出力を行う機能処理ルーチンを呼び出す命令である場合に前記実行手段による前記プログラムの実行を停止させる停止手段とを備えることを特徴とするプログラム実行制御装置。

【請求項１４】　携帯情報端末に搭載され、複数の命令からなるプログラムを取得して実行するプログラム実行制御装置であって、

通信路からプログラムを取得する取得手段と、
取得したプログラムを実行する実行手段と、
実行中のプログラムが次に実行しようとする命令を監視し、前記命令が前記携帯情報端末が備える機能処理ルーチンであって前記携帯情報端末が備える入力デバイスからのデータ取得を行う機能処理ルーチンを呼び出す命令である場合に前記実行手段による前記プログラムの実行を停止させる停止手段とを備えることを特徴とするプログラム実行制御装置。

【請求項１５】　前記プログラム実行制御装置はさらに、
前記停止手段によって前記プログラムの実行が停止した場合に、停止した旨をユーザに通知する通知手段を備えることを特徴とする請求項１～１４のいずれか１項に記載のプログラム実行制御装置。

【請求項１６】　前記プログラム実行制御装置はさらに、
前記停止手段によって前記プログラムの実行が停止した場合に、ユーザによる入力を受け付けて前記入力に応じて停止を解除する停止解除手段を備えることを特徴とする請求項１～１５のいずれか１項に記載のプログラム実行制御装置。

【請求項１７】　プログラム実行機能を有する機器に、前記機器の特定の資源を利用する機能群のうち自らが使用する機能を示す使用機能情報が付加されたオブジェクトプログラムを取得して実行するプログラム実行制御処理を、行わせる制御プログラムを記録した記録媒体であって、
前記プログラム実行制御処理は、
通信路からオブジェクトプログラムを取得する取得ステップと、
取得したオブジェクトプログラムを実行する実行ステップと、
前記使用機能情報に基づく判断を行い、判断結果がオブジェクトプログラムの実行が不適当であることを表す所定の場合に、オブジェクトプログラムの実行を停止させる停止ステップとを備えることを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、不正なプログラムの実行による被害を防ぐ技術に関し、特に携帯情報端末用のアプリケーションプログラムをダウンロードして携帯情報端末上で実行する場合におけるセキュリティ確保のための技術に関する。

【０００２】

【従来の技術】近年、通信技術、ソフトウェア技術等の進展を背景として、家電機器や携帯情報端末（以下、「家電機器等」という。）の機能の拡張等を実現するために、ＣＰＵが組み込まれた家電機器等に対するプログラムの配信サービスについての研究開発の要請が高まっている。

【０００３】家電機器等がプログラムの配信サービスに対応する機能を備えれば、家電機器等は外部のネットワーク上のサーバに用意されたアプリケーションプログラムをダウンロードすることができ、必要な時にそのアプリケーションプログラムを実行することができるようになる。従って、家電機器等のユーザは、家電機器等に最初から作り込まれている機能のみならず、後からダウンロードにより追加された種々の機能を利用することができ、例えばユーザは自己の望む機能を実現するアプリケーションプログラムを任意に選択しダウンロードして利用すること等が可能になる。

【０００４】例えば、携帯情報端末への配信サービスの対象としては通話及び通信機能に密接に関連した機能のアプリケーションプログラムやアドレス帳、ゲーム等の様々なアプリケーションプログラムが考えられる。配信サービスの対象となるアプリケーションプログラムは、基本的に、家電機器等を製造しているメーカーやその関連企業等によって作成される。また、家電機器等のメーカ等から特定機器用のアプリケーションプログラムの開発環境となるツール類等の配布を受けた、一般のプログラム開発者や企業によって作成される場合も考えられる。

【０００５】こうしてメーカーその他の者により作成されたアプリケーションプログラムを家電機器等の側でダウンロードして利用する場合を想定すると、家電機器等にはセキュリティ確保のための機能が備えられている必要がある。なぜなら、メーカー等により正当なものとして作成されたアプリケーションプログラムが悪意ある者によって、望ましくない動作を行うように不正に改変されている場合があり、また、一般のプログラム開発者等により、望ましくない動作を行うアプリケーションプログラムが提供されている場合もないとはいえないからである。

【０００６】アプリケーションプログラムによる望ましくない動作としては、機器内のデータ記憶領域内のデータを勝手に更新するような動作があり、携帯電話機等の携帯情報端末においては内部に記憶されている電話番号、メールアドレスその他のプライバシーに関わる情報（以下、「個人情報」という。）の読み出しや外部への発呼等も、ユーザの意思に沿わない場合は望ましくない動作といえる。

【０００７】ところで、従来パーソナルコンピュータ等の分野ではインターネットからダウンロードしたアプリケーションプログラムの実行時におけるセキュリティ確保を実現する仕組みとして、Ｊａｖａ（登録商標）仮想マシンのコードベリファイアという機構がある。コードベリファイアは、アプリケーションプログラムであるＪａｖａクラスファイルを解釈実行する前に、そのフォーマットや命令列を検査し、静的制約や構造体制約に従っ

て、ダウンロードされたＪａｖａクラスファイルが実行中に危険な動作を行わないことを保証する。このコードベリファイアについては、「Ｔｈｅ　Ｊａｖａ　Ｖｉｒｔｕａｌ　Ｍａｃｈｉｎｅ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ」（Ｔｉｍ　Ｌｉｎｄｈｏｌｍ、Ｆｒａｎｋ　Ｙｅｌｌｉｎ著、Ａｄｄｉｓｏｎ－Ｗｅｓｌｅｙ、１９９７年）に詳しく記述されている。

【０００８】

【発明が解決しようとする課題】しかしながら、このコードベリファイアによるアプリケーションプログラムの正当性の検査は、複雑な処理であるため多大な処理ステップを要する。従って、Ｊａｖａクラスファイルを実行するためにはクロック周波数が最低でも１００ＭＨｚ以上の高性能のＣＰＵや2ＭＢｙｔｅ～4ＭＢｙｔｅの大きなメモリの空き容量等、高価なコンピュータ資源が必要となる。これは現在においては大部分の家電機器等にとって過大な資源量であるため、コードベリファイアを備えることは、家電機器等にとって現実的なセキュリティ確保の手段とはならない。

【０００９】そこで、本発明は、家電機器等に向けて配信サービスの対象とされたアプリケーションプログラムを家電機器等がダウンロードして実行する際のセキュリティ確保を図る必要があることに鑑みてなされたものであり、家電機器等、特に携帯情報端末に適用し得るように比較的簡易な方法により、アプリケーションプログラムをダウンロードして実行する際のセキュリティ確保を実現するプログラム実行制御装置を提供することを目的とする。

【００１０】

【課題を解決するための手段】上記課題を解決するために、本発明に係るプログラム実行制御装置は、機器に搭載されており、前記機器の特定の資源を利用する機能群のうち自らが使用する機能を示す使用機能情報が付加されたプログラムを取得して、実行するプログラム実行制御装置であって、通信路からプログラムを取得する取得手段と、取得したプログラムを実行する実行手段と、前記使用機能情報に基づく判断を行い、判断結果がプログラムの実行が不適当であることを表す所定の場合に、前記実行手段によるプログラムの実行を停止させる停止手段とを備えることを特徴とする。

【００１１】上記構成により、予めプログラムに、そのプログラムが使用する機能を示す使用機能情報が付加されているので、この使用機能情報を利用することにより比較的簡易な方法でセキュリティを確保することが可能になる。即ち、使用機能情報と実際のプログラムの動作とを比べることによりそのプログラムが改竄されていることを検出することや、使用機能情報を参照することにより、使用を禁止すべき機能をそのプログラムが使用するかどうかを検出することが簡易な構成で実現できるようになる。

【００１２】

【発明の実施の形態】以下、本発明の実施の形態であるプログラム実行装置について説明する。

＜構成＞図１は、本発明の実施の形態に係るプログラム実行装置３００等の構成図である。

【００１３】同図には、携帯電話機に備えられるプログラム実行装置３００の他に、プログラム実行装置３００において実行されるオブジェクトプログラム１００と、オブジェクトプログラム１００を生成するプログラム生成装置２００とをも示している。

＜プログラム生成装置＞プログラム生成装置２００は、実行時使用機能情報を付加したオブジェクトプログラムを生成する装置であり、コンピュータ上で動作するコンパイラ及びリンカである。このオブジェクトプログラムはプログラム実行装置３００上で動作する実行形式のプログラムを意味するものであり、アプリケーションプログラムである。なお、実行時使用機能情報については後述する。

【００１４】プログラム生成装置２００は、従来のコンパイラ及びリンカと同等の機能に加えて実行時使用機能情報を生成する機能を有し、実行時使用機能情報を生成する機能を実現するために機能ＩＤテーブル２０１と実行時使用機能情報生成部２０２とを備える。図３は、機能ＩＤテーブルのデータ構造及び内容例を示す図である。

【００１５】機能ＩＤテーブルは機能ＩＤ４０１とライブラリ番号４０２との組の集合からなるテーブルである。同図に示した内容例では、０ｘ０００１という機能ＩＤは６というライブラリ番号が対応付けられている。ここで、機能ＩＤ４０１はプログラム実行装置３００上で動作するオブジェクトプログラムが利用する各機能の識別子である。なお、運用上の前提としてプログラム実行装置３００上で動作するオブジェクトプログラムが利用できる各機能は予め分類整理され、それぞれに識別子が定められていることとする。

【００１６】また、ライブラリ番号４０２は、オブジェクトプログラム内で呼び出しが可能なライブラリプログラムの番号である。即ち、オブジェクトプログラムの動作環境であるプログラム実行装置３００上に用意されたライブラリプログラムの番号である。なお、ライブラリ呼び出しにより使用し得る機能は、例えば無線インタフェースへのデータ出力機能、ディスプレイへのデータ出力機能、音声出力回路へのデータ出力機能、無線インタフェースからのデータ入力機能、ボタンからのデータ入力機能等がある。図３の内容例では括弧内に機能ＩＤの意味する機能を便宜上付記している。

【００１７】実行時使用機能情報生成部２０２は、プログラム生成装置２００が従来のコンパイラ及びリンカと同等の機能によりオブジェクトプログラムを生成した後に、生成されたオブジェクトプログラム中で呼び出して

いるライブラリプログラムを検索して機能ＩＤテーブル２０１に照らして機能ＩＤを得ることにより、オブジェクトプログラムが使用する機能を示す実行時使用機能情報を生成し、そのオブジェクトプログラムに付加する。

【００１８】図４は、オブジェクトプログラムに付加される実行時使用機能情報のデータ構造及び内容例を示す図である。実行時使用機能情報は、オブジェクトプログラムがライブラリ呼び出しによって使用し得る全ての機能について、機能ＩＤ毎に実際にその情報の付加先となるオブジェクトプログラムが使用しているか否かを示すフラグ５０２を対応付けた情報である。フラグ５０２は、０ｘ００が使用しない旨を示し、０ｘ０１が使用する旨を示す。

【００１９】同図の内容例は、例えば機能ＩＤが０ｘ０００１の機能は使用されず、機能ＩＤが０ｘ０００２の機能は使用されることを示している。このようなプログラム生成装置２００によって生成されたオブジェクトプログラム１００は図１に示すように、実行プログラム１０１と実行時使用機能情報１０２とから構成されるものとなる。ここで、実行プログラム１０１は、通常のオブジェクトプログラム自体であり、プログラム実行装置３００上で解釈実行されるものである。

【００２０】オブジェクトプログラム１００は、例えばＪａｖａクラスファイルであり、実行時使用機能情報１０２は、Ｊａｖａクラスファイル中にアトリビュート情報として置かれる。なお、Ｊａｖａクラスファイルはアトリビュート情報を付加することができるものである。またアトリビュート情報は識別番号を設定できるものであり、特定のＪａｖａ仮想マシンとの間での取決めに従ってその内容を定めることができる。つまり、特定の識別番号のアトリビュート情報を解釈できるようにＪａｖａ仮想マシンを構築しておくことが可能になっている。また、Ｊａｖａ仮想マシンの仕様では、その特定の識別番号のアトリビュート情報を解釈できないＪａｖａ仮想マシンはそのアトリビュート情報を読み飛ばすこととされている。

【００２１】ここでは、実行時使用機能情報１０２は、プログラム実行装置３００がオブジェクトプログラム１００を取得して実行する際にメモリにロードした時点でプログラム実行装置３００によって参照され得るものであることとする。

＜プログラム実行装置＞プログラム実行装置３００は、携帯電話機内に備えられ、オブジェクトプログラム１００を取得して実行する装置であり、オペレーティングシステム及びＪａｖａ仮想マシンを含むものである。

【００２２】プログラム実行装置３００は、図１に示すようにプログラム解釈実行部３０１、使用機能監視部３０２、実行時使用機能監視検査部３０３、使用禁止テーブル３０４、実行時使用機能禁止検査部３０５、監視禁止検査部３０６、ユーザ通達部３０７、プログラム実行許可判定部３０８、ユーザ禁止指定入力部３０９及び機能ＩＤテーブル３１０を有する。これらプログラム解釈実行部３０１その他各部は、基本的に携帯電話機のメモリに備えられた制御プログラムがＣＰＵにより実行されることによりその機能を発揮する。

【００２３】ここで、プログラム解釈実行部３０１は、実行プログラム１０１を解釈実行するものであり、基本的には従来のＪａｖａ仮想マシンと同様にＪａｖａクラスファイルを逐次解釈実行するいわゆるインタプリタである。但し、プログラム解釈実行部３０１は通常のインタプリタとしての機能に加えて、実行プログラム１０１の解釈実行中に、実行時使用機能監視検査部３０３、実行時使用機能禁止検査部３０５又は監視禁止検査部３０６の通知を受けることにより解釈実行を停止できる機能を有している。

【００２４】使用機能監視部３０２は、プログラム解釈実行部３０１が実行プログラム１０１を解釈実行しているときに、次に実行されようとしているＪａｖａバイトコード（以下、「命令」ともいう。）を監視して、予め定められている機能のうちいずれかが使用されようとした場合に、その使用されようとした機能についての機能ＩＤを出力する。即ち、使用機能監視部３０２は、実行プログラム１０１を逐次解釈しているプログラム解釈実行部３０１から、次にプログラムカウンタが指す位置の命令、つまり次に実行しようとしている命令を通知され、機能ＩＤテーブル３１０を参照して後述する監視処理を行うことにより、その命令に対応する機能ＩＤを得て、機能ＩＤを出力する。

【００２５】実行時使用機能監視検査部３０３は、使用機能監視部３０２から出力された機能ＩＤと実行時使用機能情報１０２とを入力とし、実行時使用機能情報１０２において使用しない旨のフラグに対応付けられている機能ＩＤが使用機能監視部３０２から出力された場合には、実行プログラム１０１の解釈実行を停止するようにプログラム解釈実行部３０１に伝える。

【００２６】使用禁止テーブル３０４は、プログラム実行装置３００上で動作するアプリケーションプログラムに使用され得る全ての機能それぞれについて、ダウンロードしたオブジェクトプログラム１００の実行プログラム１０１に対してその機能を使用することを許可しているか禁止しているかを示す情報を記録したテーブルである。

【００２７】図５は、使用禁止テーブル３０４のデータ構造及び内容例を示す図である。同図に示すように使用禁止テーブルは機能ＩＤ６０１とその機能ＩＤで示される機能の使用が許可されているか禁止されているかを示すフラグ６０２との組の集合からなるテーブルである。機能ＩＤ６０１は、アプリケーションプログラムに使用され得る機能を区分して、区分された各機能に一意となるように識別子を割り当てたものであり、その各機能に

は、アプリケーションプログラムから呼び出されるライブラリに対応した機能が含まれ、さらにロード命令やストア命令に対応する機能が含まれる。つまり、使用禁止テーブルには、機能ＩＤテーブル又は実行時使用機能情報に含まれる機能ＩＤを全て包含した上にロード命令やストア命令に対応する機能ＩＤが含まれる。

【００２８】フラグ６０２は、０ｘ００が使用を禁止する旨を示し、０ｘ０１が使用を許可する旨を示す。同図に示す内容例では、例えば、ロード命令に対応するものとして、個人情報領域からのデータ読出を意味する０ｘ０１０１という機能ＩＤの機能と、システム領域からのデータ読出を意味する０ｘ０１０２という機能ＩＤの機能と、ストア命令に対応するものとして、個人情報領域へのデータ書込を意味する０ｘ０２０１という機能ＩＤの機能と、システム領域へのデータ書込を意味する０ｘ０２０２という機能ＩＤの機能とは、使用が禁止されていることを示している。なお、個人情報領域及びシステム領域については後に説明する。

【００２９】また、実行時使用機能禁止検査部３０５は、実行時使用機能情報１０２と使用禁止テーブル３０４とを参照して、これらを比較することにより、実行時使用機能情報１０２において使用する旨のフラグに対応付けられている機能ＩＤと同一の機能ＩＤが使用禁止テーブル３０４においては使用を禁止する旨のフラグに対応付けられている場合には、実行プログラム１０１の解釈実行を停止するようにプログラム解釈実行部３０１に伝える。

【００３０】監視禁止検査部３０６は、使用機能監視部３０２から出力された機能ＩＤと使用禁止テーブル３０４とを入力とし、使用禁止テーブルにおいて使用を禁止する旨のフラグに対応付けられている機能ＩＤが使用機能監視部３０２から出力された場合には、実行プログラム１０１の解釈実行を停止するようにプログラム解釈実行部３０１に伝える。

【００３１】ユーザ通達部３０７は、プログラム解釈実行部３０１による実行プログラム１０１の解釈実行が停止した旨を携帯電話機のディスプレイに表示するよう制御して、プログラムの実行停止をユーザに通達するものである。プログラム実行許可判定部３０８は、ユーザ通達部３０７とともに解釈実行の停止時におけるユーザインタフェースを構成するものであり、実行プログラム１０１の解釈実行の停止の旨をユーザ通達部３０７がディスプレイに表示するよう制御した場合に、実行プログラム１０１の停止を解除するか又は実行プログラム１０１の実行を終了するかのユーザによる指定を携帯電話機の各種ボタン等を通じて受け付け、その指定に応じてプログラム解釈実行部３０１に対して停止の解除又は終了の指示を伝える。

【００３２】ユーザ禁止指定入力部３０９は、使用禁止テーブル３０４の内容の変更についての入力を携帯電話機の各種ボタン等を通じてユーザから受け付け、その入力に応じて使用禁止テーブル３０４を更新する。ユーザ禁止指定入力部３０９が存在することによって、ユーザはダウンロードしたアプリケーションプログラムにより特定の機能が使用されることを許可するか禁止するかを指定することができる。

【００３３】また、機能ＩＤテーブル３１０は、機能ＩＤテーブル２０１と同一内容のテーブルであり、図３に示す構造を有するテーブルである。なお、プログラム実行装置３００は、無線基地局を介して通信によりアプリケーションプログラムを取得、即ちダウンロードして携帯電話機に備えられたメモリに格納する機能を有する。

【００３４】図２は、プログラム実行装置３００を備える携帯電話機３２０とダウンロード対象のオブジェクトプログラムとの関係を示す図である。公衆網に接続されたコンピュータであるプログラム格納サーバ２５０には携帯電話機にダウンロードされることを目的としてプログラム生成装置２００を備えるプログラム生成系から提供されたオブジェクトプログラム１００が格納されている。プログラム実行装置３００を備える携帯電話機３２０は、無線基地局２６０と無線通信することにより無線基地局２６０を介してプログラム格納サーバ２５０に格納されているオブジェクトプログラム１００をダウンロードすることができる。

【００３５】＜メモリ構造＞ここで、プログラム実行装置３００が実行するアプリケーションプログラムがアクセスし得るメモリについて説明する。メモリは、個人情報を記録するための個人情報領域と、オペレーティングシステムやインタプリタ機能の実行に必要な情報を記録するためのシステム領域と、その他の領域とに分けられる。

【００３６】図６は、メモリ内の領域の分類を示した図である。同図に示すようにメモリは０ｘ０００００番地から０ｘ３ＦＦＦ番地までがシステム領域であり、０ｘ４０００番地から０ｘ７ＦＦＦ番地までが個人情報領域であり、０ｘ８０００番地から０ｘＦＦＦＦ番地までがシステム領域でも個人情報領域でもないその他の領域である。

【００３７】つまり、携帯電話機に最初から内蔵されたアプリケーションプログラムによって、個人情報は個人情報領域に記録されるようになっており、またプログラム実行装置３００はシステム領域にアクセスして処理の実行に必要なデータの記録及び読み出しを行うものである。図７は、個人情報の内容の具体例を示す図である。同図に示すように、個人情報は、人物名や電話番号等の個人のプライバシーに関わる情報を含んでいる。従って、この個人情報領域に格納されている個人情報は不正なアクセスから特に保護されるべきである。

＜動作＞以下、上述の構成を備えるプログラム実行装置３００の動作について説明する。

【００３８】＜解釈実行動作＞図８は、プログラム実行装置３００がダウンロードしたオブジェクトプログラムを解釈実行する際における処理手順を示すフローチャートである。プログラム実行装置３００は、無線基地局との通信によりオブジェクトプログラム１００をダウンロードし、メモリに格納した後、解釈実行を始める。

【００３９】プログラム解釈実行部３０１が実行プログラム１０１の解釈実行を行うに際して、まず実行時使用機能禁止検査部３０５は、Ｊａｖａクラスファイルの特定の識別番号で識別されるアトリビュート情報を参照することにより実行時使用機能情報１０２にアクセスして、実行時使用機能情報１０２と使用禁止テーブル３０４とを比較し（ステップＳ１０１）、実行時使用機能情報１０２において使用する旨のフラグと対応付けられている機能ＩＤのうちいずれかが、使用禁止テーブルにおいて使用が禁止されている旨のフラグと対応付けられている機能ＩＤと一致するか否かを判定する（ステップＳ１０２）。

【００４０】ステップＳ１０２において一致すると判定した場合には、実行時使用機能禁止検査部３０５はプログラム解釈実行部３０１及びユーザ通達部３０７に停止を通知しプログラム実行装置３００は解釈実行停止処理を行い（ステップＳ１０３）、一致しないと判定した場合にはステップＳ１０３をスキップし、続いて監視処理を行う（ステップＳ１０４）。なお、解釈実行停止処理については後に説明する。

【００４１】ここで、監視処理を説明する。図９は、使用機能監視部３０２による監視処理を示すフローチャートである。プログラム解釈実行部３０１はプログラムカウンタを参照して次に実行する命令を得て使用機能監視部３０２に伝える（ステップＳ２０１）。使用機能監視部３０２は、その命令がａｌｏａｄ等のデータ読出命令であるか否かを判定し（ステップＳ２０２）、データ読出命令であれば、その命令のオペランドに基づいて、メモリ内の読出対象となる位置である読出アドレスを取得する（ステップＳ２０３）。読出アドレスがレジスタ等によって指定されている場合であっても、ステップＳ２０３の実行の際におけるそのレジスタ等の内容値を参照することによって実際の読出アドレスを取得する。

【００４２】読出アドレスを取得した後、その読出アドレスはシステム領域内を指すものであるか否かを判定し（ステップＳ２０４）、システム領域内を指すものであれば０ｘ０１０２という機能ＩＤを実行時使用機能監視検査部３０３及び監視禁止検査部３０６に伝えて監視処理を終了する（ステップＳ２０５）。ステップＳ２０４においてシステム領域内を指すものでなければ、読出アドレスは個人情報領域内を指すものであるか否かを判定し（ステップＳ２０６）、個人情報領域内を指すものであれば０ｘ０１０１という機能ＩＤを実行時使用機能監視検査部３０３及び監視禁止検査部３０６に伝えて監視処理を終了する（ステップＳ２０７）。

【００４３】ステップＳ２０６において個人情報領域内を指すものでなければ、０ｘ０００Ｏという機能ＩＤを実行時使用機能監視検査部３０３及び監視禁止検査部３０６に伝えて監視処理を終了する（ステップＳ２０８）。得た命令がデータ読出命令でない場合には（ステップＳ２０２）、使用機能監視部３０２はその命令がａｓｔｏｒｅ等のデータ書込命令であるか否かを判定し（ステップＳ２０９）、データ書込命令であれば、その命令のオペランドに基づいて、メモリ内の書込対象となる位置である書込アドレスを取得する（ステップＳ２１０）。書込アドレスがレジスタ等によって指定されている場合であっても、ステップＳ２１０の実行の際におけるそのレジスタ等の内容値を参照することによって実際の書込アドレスを取得する。

【００４４】書込アドレスを取得した後、その書込アドレスはシステム領域内を指すものであるか否かを判定し（ステップＳ２１１）、システム領域内を指すものであれば０ｘ０２０２という機能ＩＤを実行時使用機能監視検査部３０３及び監視禁止検査部３０６に伝えて監視処理を終了する（ステップＳ２１２）。ステップＳ２１１においてシステム領域内を指すものでなければ、書込アドレスは個人情報領域内を指すものであるか否かを判定し（ステップＳ２１３）、個人情報領域内を指すものであれば０ｘ０２０１という機能ＩＤを実行時使用機能監視検査部３０３及び監視禁止検査部３０６に伝えて監視処理を終了する（ステップＳ２１４）。

【００４５】ステップＳ２１３において個人情報領域内を指すものでなければ、０ｘ０００Ｏという機能ＩＤを実行時使用機能監視検査部３０３及び監視禁止検査部３０６に伝えて監視処理を終了する（ステップＳ２１５）。得た命令がデータ書込命令でない場合には（ステップＳ２０９）、使用機能監視部３０２はその命令がｉｎｖｏｋｅ　ｖｉｒｔｕａｌ等のライブラリ呼出命令であるか否かを判定し（ステップＳ２１６）、ライブラリ呼出命令であれば、その命令のオペランドからライブラリ番号を得て、そのライブラリ番号に対応する機能ＩＤを機能ＩＤテーブル３１０を参照することにより取得して、その機能ＩＤを実行時使用機能監視検査部３０３及び監視禁止検査部３０６に伝えて監視処理を終了する（ステップＳ２１７）。

【００４６】また、ステップＳ２１６においてライブラリ呼出命令でなければ、使用機能監視部３０２は、０ｘ０００Ｏという機能ＩＤを実行時使用機能監視検査部３０３及び監視禁止検査部３０６に伝えて監視処理を終了する（ステップＳ２１８）。なお、使用機能監視部３０２から出力される機能ＩＤは、ライブラリ呼出命令に対応する機能ＩＤかそれ以外の命令に対応する機能ＩＤかが識別できるようになっており、ここでは、機能ＩＤのうち上位８ビットが０ｘ００であるものがライブラリ呼

出命令に対応するものであることとしている。

【００４７】以下、図８に即した説明に戻る。上述した監視処理（ステップＳ１０４）の後、実行時使用機能監視検査部３０３は監視処理の結果として使用機能監視部３０２から出力された機能ＩＤと、実行時使用機能情報１０２との比較検査を行い（ステップＳ１０５）、実行プログラム１０１中の次に実行される命令によって使用される機能の機能ＩＤ即ち監視処理の結果として出力された機能ＩＤと同一の機能ＩＤが実行時使用機能情報１０２において使用しない旨のフラグと対応付けられているか否かを判定する（ステップＳ１０６）。ステップＳ１０６は、実行時使用機能情報１０２によって使用しないと宣言している機能を、実際の実行に際しては使用しようとしていたか否かを判定するという意味を持つ。

【００４８】ステップＳ１０６において監視処理の結果として出力された機能ＩＤが実行時使用機能情報１０２において使用しない旨のフラグと対応付けられている機能ＩＤであった場合に限り、実行時使用機能監視検査部３０３はプログラム解釈実行部３０１及びユーザ通達部３０７に停止を通知しプログラム実行装置３００は解釈実行停止処理を行い（ステップＳ１０７）、その他の場合にはステップＳ１０７をスキップし、その後に監視処理の結果として出力された機能ＩＤと使用禁止テーブルとの比較検査を監視禁止検査部３０６が行う（ステップＳ１０８）。

【００４９】ステップＳ１０８においては監視禁止検査部３０６は監視処理の結果として出力された機能ＩＤと同一の機能ＩＤが使用禁止テーブルにおいて使用を禁止する旨のフラグと対応付けられているか否かを判定する（ステップＳ１０９）。この判定の結果、監視処理の結果として出力された機能ＩＤが使用禁止テーブルにおいて使用を禁止する旨のフラグと対応付けられている機能ＩＤであった場合に限り監視禁止検査部３０６はプログラム解釈実行部３０１及びユーザ通達部３０７に停止を通知し解釈実行停止処理を行い（ステップＳ１１０）、その他の場合にはステップＳ１１０をスキップする。

【００５０】続いて、監視処理の対象となった命令即ち次に実行されるべき命令をプログラム解釈実行部３０１が解釈実行する（ステップＳ１１１）。プログラム解釈実行部３０１による実行プログラム１０１の全ての処理の解釈実行が終了するまでステップＳ１０４からＳ１１１の処理が繰り返され、全ての処理の解釈実行が終了するとプログラム実行装置の動作も終了する（ステップＳ１１２）。

【００５１】以下、解釈実行停止処理について説明する。図１０は、解釈実行停止処理を示すフローチャートである。停止の通知を受けたプログラム解釈実行部３０１は実行プログラムの解釈実行を停止するように内部の変数等による制御状態を設定し（ステップＳ３０１）、ユーザ通達部３０７は解釈実行が停止されたことをユーザに通達する（ステップＳ３０２）。

【００５２】このステップＳ３０２におけるユーザ通達部３０７の制御によりディスプレイに表示される画面は、例えば図１１に示すものとなる。この画面はファイル名がｍａｚｅ．ｃｊである実行プログラム１０１の実行が停止された旨を示すとともにユーザに対して実行の継続を指示する場合に用いるボタンを知らせるものである。

【００５３】ユーザ通達部３０７によるユーザへの停止の通達の後にプログラム実行許可判定部３０８はユーザの入力を受け付け解釈し（ステップＳ３０３）、実行プログラム１０１の解釈実行を継続する旨の指示の入力であるか否かを判断する（ステップＳ３０４）。ステップＳ３０４において解釈実行の継続の指示と判断した場合にはプログラム実行許可判定部３０８はプログラム解釈実行部３０１に解釈実行の停止の解除を指示し、これを受けてプログラム解釈実行部３０１は解釈実行の停止を解除するように制御状態を設定する（ステップＳ３０５）。このステップＳ３０５により実行プログラム１０１は引き続いて解釈実行されるものとなる。

【００５４】またステップＳ３０４において解釈実行の継続の指示でないと判断した場合にはプログラム実行許可判定部３０８はプログラム解釈実行部３０１に解釈実行の終了を指示し、これを受けてプログラム解釈実行部３０１は解釈実行を終了するように制御状態を設定する。（ステップＳ３０６）。このステップＳ３０６により実行プログラム１０１は以後解釈実行されることはなくなり、プログラム実行装置３００の動作は終了する。

【００５５】＜使用禁止テーブル更新動作＞プログラム実行装置３００は、プログラムの解釈実行中以外の時において使用禁止テーブルの更新を行う機能を有する。この機能は、ユーザにより例えば携帯電話機の特定のボタンが押下された場合等の所定操作に対応して実行されるものであり、所定操作が行われるとユーザ禁止指定入力部３０９は携帯電話機のディスプレイに図１２に示すような使用禁止機能選択画面を表示するよう制御して、ユーザによる使用禁止機能の指定に関する入力を受け付ける。

【００５６】ユーザ禁止指定入力部３０９は、図１２に示すように機能項目等を表示し、ユーザの特定のボタン操作に応じて機能項目の表示をスクロールさせ、また「１」又は「０」のボタン入力を受け付けると強調表示されている機能項目で表しているところの機能の使用を許可又は禁止とするように使用禁止テーブル３０４を更新する。

【００５７】これにより、使用を禁止する機能をユーザが定めることができるようになる。例えば個人情報を読み出されても構わないと考えるユーザであれば、個人情報領域からのデータ読出の機能の使用を許可するように使用禁止テーブル３０４を変更することが可能になる。

＜補足＞以上、本発明に係るプログラム実行装置について実施の形態を用いて説明したが、本発明は実施の形態に示したものに限られることはない。即ち、

（１）本実施の形態では、個人情報が格納されるメモリ内の領域等はそのアドレスが固定的に定められているものとしたが、特定サイズのデータ毎にフラグを付加することとし、そのフラグにより個人情報であるかその他の情報であるかを識別できるようにしておくこととすれば、個人情報はメモリ空間内の任意のアドレスに分散して格納することも可能となる。つまり固定的でない特定サイズの個人情報領域が複数存在することとしてもよい。

【００５８】図１３は、メモリ内に個人情報であるデータと個人情報以外であるデータがフラグによって識別可能となるように格納されている例を示す図である。同図ではフラグは０か１の値をとり、フラグが１であれば個人情報であることを示している。このような場合には、監視処理における読出アドレス又は書込アドレスが個人情報領域内か否かの判断（ステップＳ２０６、Ｓ２１３）は、そのアドレスが指すデータに付加されたフラグが０か１かに基づいて行うこととする必要がある。なお、個人情報とシステムデータとその他のデータとを識別するようなフラグを特定サイズのデータ毎に付加することとすれば、同様の方法によりシステム領域内か否かの判断（ステップＳ２０４、Ｓ２１１）をも行うこととしてもよい。

（２）本実施の形態において使用禁止テーブル３０４や実行時使用機能情報１０２等において示した機能の区分は単なる一例であり、他の区分であってもよい。また、機能ＩＤテーブルはライブラリ呼出命令に対応する機能を列挙したテーブルとなっており、実行時使用機能情報１０２にはライブラリ呼出命令により実行され得る全ての機能について、使用するかしないかのフラグを対応付けた情報であるとしたが、ライブラリ呼出命令でない他の特定の命令により実行される機能についての情報を盛り込むこととしてもよい。但し、機能ＩＤテーブル及び実行時使用機能情報に機能ＩＤが含まれる機能は、その機能の使用の有無の確認がプログラムの実行前において簡易に行えるものとするのが望ましい。

【００５９】なお、通常、プログラム実行装置が搭載された機器側に用意されたライブラリをオブジェクトプログラムが呼び出すことにより使用できる機能は、その機器の特定の資源を利用する機能であるため、機能ＩＤテーブルはライブラリ毎に対応する機能を列挙したテーブルであることとすると、オブジェクトプログラムが危険動作を行うことを回避するというセキュリティ確保の目的を達成するためには適したものとなるといえる。

（３）本実施の形態では、使用禁止テーブル（図５参照）により無線インタフェースへのデータ出力や無線インタフェースからのデータ入力を禁止する例を示したが、これらを必ずしも禁止しなければならないことはなく、また他の回路へのデータ入出力を禁止することとしてもよいし、その他のライブラリ呼出によって実現される機能を禁止してもよい。また、無線インタフェースからのデータ入力及び無線インタフェースへのデータ出力の機能を禁止する代わりに外部への発呼機能、即ち電話をかける機能を禁止することとしてもよい。

【００６０】なお、無線インタフェースを通じてのデータ入出力を禁止することは、ユーザが知らない内に外部と通信することを防ぐ意味において実用上有用である。また、例えばボタン、スイッチ、ダイヤル、マウス、トラックボール、ジョイスティック、キーボード、マイク、カメラ、センサ等の広い意味での入力デバイスからのデータ取得を禁止することや、ディスプレイ、ＬＥＤ、ランプ、スピーカー、バイブレータ等の広い意味での出力デバイスへのデータ出力を禁止することは、盗聴等の不正な情報取得の防止や、迷惑な出力の防止の面において有用な場合がある。

【００６１】また、本実施の形態では、使用禁止テーブルにより個人情報領域からのデータ読出、システム領域からのデータ読出、個人情報領域へのデータ書込及びシステム領域へのデータ書込を禁止する例を示したが、これらを必ずしも禁止しなければならないことはなく、またその他の特定の命令の実行を禁止するようにしてもよい。なお、個人情報へのアクセスを禁止することは、プライバシー保護等の面から実用上有用である。

（４）本実施の形態において図１０のステップＳ３０３で示したユーザの入力は、ボタンに限らず、他の入力デバイスを介してなされることとしてもよい。また、ステップＳ３０３においては、予め定められた取決めに従って、ユーザが操作をなさなかったことを特定の指定を入力したものと解釈することにしてもよい。例えば、実行プログラムが停止した旨がディスプレイに表示されてから３０秒間何も入力しなければ、プログラム実行許可判定部３０８はその実行プログラムの解釈実行の継続を行わないという指定がユーザによりなされたと解釈することとしてもよい。

（５）本実施の形態において図２に示したオブジェクトプログラム１００を携帯電話機がダウンロードする際には、そのオブジェクトプログラム１００の配信側であるプログラム格納サーバ２５０の正当性を確認するために、相互認証等を行うこととしてもよい。

【００６２】また、本実施の形態では、プログラム実行装置３００は携帯電話機に備えられるものとしたが、これに限定されるものではなく、他の家電機器や携帯情報端末に適用されるものであることとしてもよい。また、プログラム実行装置３００の実行対象となるオブジェクトプログラムの取得経路も図２に示したものに限定されることはなく、例えばＢｌｕｅｔｏｏｔｈ、ＨｏｍｅＲＦ等に定められているような方法でオブジェクトプログ

ラムが伝送されることとしてもよい。

（６）本実施の形態では、ダウンロードするアプリケーションプログラム、即ちオブジェクトプログラムはＪａｖａクラスファイルであることとしたが、これに限定されることはなく、機械語プログラムであることとしてもよい。機械語プログラムの場合にはプログラム解釈実行部３０１はＣＰＵであることとし、使用機能監視部３０２はいわゆるプログラムカウンタに相当するレジスタが変化する毎に各レジスタ及びメモリを参照して次に実行される命令を監視することとしてもよい。

（７）本実施の形態で示した図１０のステップＳ３０６は、実行プログラムの解釈実行を終了するだけであるが、ステップＳ３０６はさらに、終了した実行プログラムとこれに付随する実行時使用機能情報とを携帯電話機の記憶装置内から削除することとしてもよい。また、ダウンロードしたオブジェクトプログラムをプログラム実行装置３００が実行することによって図８のステップＳ１１２でＹＥＳの分岐に進んだ場合において、次の処理を追加することとしてもよい。その処理は、実行が完了したオブジェクトプログラムを次回以後は通常のインタプリタ等の実行対象とするための処理であり、例えばそのオブジェクトプログラムのファイル名を安全であるアプリケーションプログラムのリストに登録する処理や、Ｊａｖａクラスファイルのアトリビュート情報に安全である旨の情報を記録する処理等が考えられる。なお、オブジェクトプログラムが通常のインタプリタ等の実行対象となるということの意味は、使用機能監視等の不正な機能の実行を抑止するための処理を行うことなく実行されるということである。従って、例えば安全であるアプリケーションプログラムのリストに登録されているオブジェクトプログラム、安全である旨の情報が付加されたオブジェクトプログラム等の安全性が保証されたプログラムについては、プログラム実行装置３００が不正な機能の実行を抑止することなく従来のインタプリタと同様の機能のみを用いてそのプログラムを実行することとしてもよい。

（８）本実施の形態で示したプログラム生成装置２００は、オブジェクトプログラムを生成した後に、そのオブジェクトプログラムが使用する機能の機能ＩＤを検索して実行時使用機能情報を生成することとしたが、Ｃ言語やＪａｖａ言語等で記述されたソースプログラムをオブジェクトプログラムに翻訳する過程において、そのオブジェクトプログラム使用することになる機能を把握して実行時使用機能情報を生成するものであってもよい。

【００６３】また、プログラム生成装置２００は、オブジェクトプログラムに含める実行時使用機能情報を、配信経路における改竄から保護するために暗号化することとしてもよい。この場合にはプログラム実行装置３００側では実行時使用機能情報を復号して参照するようにする必要がある。

（９）本実施の形態では、個人情報領域には、人物名、電話番号、メールアドレスその他の個人情報が含まれることとして、ダウンロードしたオブジェクトプログラムによる個人情報領域へのデータ書込又は個人情報領域からのデータ読出の機能の使用を禁止することとし、またユーザは使用禁止テーブルの更新によりこれらの機能の使用を禁止から許可に変更することができることとした。このように個人情報をひとまとめに管理するのではなく、個人情報を複数の種別に区分して種別毎に管理することとしてもよい。即ち、個人情報領域を第１種個人情報領域、第２種個人情報領域、第３種個人情報領域等と区分して、この区分された領域毎に、ダウンロードしたオブジェクトプログラムによるデータ書込や読出の禁止又は許可の制御を行うこととしてもよい。

（１０）本実施の形態において実行プログラムの解釈実行に関して用いた「停止」という用語は、図８のステップＳ１０１、Ｓ１０２に示した処理等を実行プログラムの起動前に行う場合には解釈実行の「抑止」を意味する。なお、実行プログラムが複数のモジュールから構成される場合においてプログラム実行装置３００が各モジュールを必要時に動的にメモリにロードして実行するとしてもよく、この場合にはロード直後にステップＳ１０１～Ｓ１０３の処理を行うこととしてもよいので、必ずしも実行プログラムの起動前に解釈実行を抑止するとは限らず、実行プログラムの実行中に解釈実行を停止するケースも起り得る。

（１１）本実施の形態において図１１に示した画面には、実行プログラムがどの機能を使用することになるために停止されたか等、停止を解除させるべきか否かのユーザによる判断に有用な情報を付加することとしてもよい。

（１２）本実施の形態におけるプログラム実行装置３００の処理手順（図８～図１０に示した手順等）を、プログラム実行機能を有する家電機器、携帯情報端末等に実行させるためのコンピュータプログラムを、記録媒体に記録し又は各種通信路等を介して、流通させ頒布することもできる。このような記録媒体には、ＩＣカード、光ディスク、フレキシブルディスク、ＲＯＭ等がある。流通、頒布されたコンピュータプログラムは、家電機器、携帯情報端末等にインストール等されることにより利用に供され、家電機器、携帯情報端末等は、前記コンピュータプログラムを実行して本実施の形態で示したようなプログラム実行装置を実現する。

【００６４】

【発明の効果】以上の説明から明らかなように、本発明に係るプログラム実行制御装置は、機器に搭載されており、前記機器の特定の資源を利用する機能群のうち自らが使用する機能を示す使用機能情報が付加されたプログラムを取得して、実行するプログラム実行制御装置であって、通信路からプログラムを取得する取得手段と、取

得したプログラムを実行する実行手段と、前記使用機能情報に基づく判断を行い、判断結果がプログラムの実行が不適当であることを表す所定の場合に、前記実行手段によるプログラムの実行を停止させる停止手段とを備えることを特徴とする。

【００６５】これにより、予めプログラムに、そのプログラムが使用する機能を示す使用機能情報が付加されているので、この使用機能情報を利用することにより比較的簡易な方法でセキュリティを確保することが可能になる。即ち、使用機能情報と実際のプログラムの動作とを比べることによりそのプログラムが改竄されていることを検出することや、使用機能情報を参照することにより、使用を禁止すべき機能をそのプログラムが使用するかどうかを検出することが簡易な構成で実現できるようになる。

【００６６】また、前記プログラムは複数の命令を含み、前記実行手段は前記プログラム中の命令を実行するものであり、前記停止手段は、実行中のプログラムにおける次に実行対象となる命令を監視し、前記命令が前記機能群のうち前記使用機能情報において使用する機能として示されていない機能を使用する命令であった場合に前記実行手段による前記プログラムの実行を停止させることとしてもよい。

【００６７】これにより、ダウンロードしたプログラムに付加されておりそのプログラムが使用する機能を示す使用機能情報と、実際の動作時にそのプログラムが使用しようとする機能を監視した結果とを比較することになるので、使用機能情報とプログラムとの相違を検出することができる。従ってプログラム生成時においては使用機能情報とプログラムとは整合するものであることを前提とすると、プログラムが通信路において不正に改竄されていることが簡単に検出できることになり、不正に改竄されたプログラムの実行による被害を防止することができるようになる。

【００６８】また、前記使用機能情報は暗号化されており、前記停止手段は前記使用機能情報を復号して参照することとしてもよい。これにより、使用機能情報が暗号化されているために通信経路においてプログラムと使用機能情報との両方を不正に書き換えることが困難になり、その結果、プログラムと使用機能情報との不整合を調べることによりプログラムの改竄は容易に検出可能となる。

【００６９】また、前記プログラム実行制御装置は、使用を禁止する機能を示す禁止機能情報を記憶する禁止機能記憶手段を備え、前記停止手段は、前記禁止機能情報に示されている使用を禁止する機能が前記使用機能情報に使用する機能として示されている場合には前記実行手段によるプログラムの実行を停止させることとしてもよい。

【００７０】これにより、危険等の理由から予め使用を禁止するものと定めている機能を、使用することが示されているプログラムの実行を停止するので、使用機能情報と禁止機能情報の比較だけの簡易な方法により安全性が確保できる。なお、ここでいう停止にはプログラム実行そのものを行わない抑止も含まれる。また、前記禁止機能情報が示す使用を禁止する機能には、少なくとも無線通信の機能が含まれることとしてもよい。

【００７１】これにより、機密情報の流出の可能性があり、また通信料金が必要となる場合もあり得る等の理由から、ダウンロードしたプログラムに自由に使用させるのは問題がある無線通信機能を使用するプログラムを停止することができる。また、前記禁止機能情報が示す使用を禁止する機能には、少なくとも出力デバイスからのデータ出力の機能が含まれることとしてもよい。

【００７２】これにより、ダウンロードしたプログラムがディスプレイにパスワード等の秘密の情報を表示する等の出力動作を行うことを防止することができる。また、前記禁止機能情報が示す使用を禁止する機能には、少なくとも入力デバイスからのデータ取得の機能が含まれることとしてもよい。これにより、ダウンロードしたプログラムがマイクを通じてデータを取得して盗聴を行う等のデータ取得動作を行うことを防止することができる。

【００７３】また、前記プログラム実行制御装置はさらに、ユーザの操作を受け付けて前記操作に応じて前記禁止機能情報を更新する禁止機能変更手段を備えることとしてもよい。これにより、危険等の理由から予め使用を禁止するものと定めている機能についてもユーザによっては危険と考えない場合もあり得ることに対応し、ダウンロードしたプログラムに使用させたくない機能をユーザが自由に設定できるようになる。

【００７４】また、本発明に係るプログラム実行制御装置は、個人情報領域を有するメモリを備える携帯情報端末に搭載され、複数の命令からなるプログラムを取得して実行するプログラム実行制御装置であって、通信路からプログラムを取得する取得手段と、取得したプログラムを実行する実行手段と、実行中のプログラムが次に実行しようとする命令を監視し、前記命令が前記個人情報領域からのデータ読出を行う命令である場合に前記実行手段による前記プログラムの実行を停止させる停止手段とを備えることを特徴とする。

【００７５】これにより、携帯情報端末に通常記憶されておりプライバシーに関わる情報である個人情報をダウンロードしたプログラムが読み出すことを防ぐことができるので、個人情報の流出を阻止できるようになる。また、本発明に係るプログラム実行制御装置は、個人情報領域を有するメモリを備える携帯情報端末に搭載され、複数の命令からなるプログラムを取得して実行するプログラム実行制御装置であって、通信路からプログラムを取得する取得手段と、取得したプログラムを実行する実

行手段と、実行中のプログラムが次に実行しようとする命令を監視し、前記命令が前記個人情報領域へのデータ書込を行う命令である場合に前記実行手段による前記プログラムの実行を停止させる停止手段とを備えることを特徴とする。

【００７６】これにより、携帯情報端末に通常記憶されておりプライバシーに関わる情報である個人情報をダウンロードしたプログラムが書き換えることを防ぐことができるようになる。また、本発明に係るプログラム実行制御装置は、携帯情報端末に搭載され、複数の命令からなるプログラムを取得して実行するプログラム実行制御装置であって、通信路からプログラムを取得する取得手段と、取得したプログラムを実行する実行手段と、実行中のプログラムが次に実行しようとする命令を監視し、前記命令が前記携帯情報端末が備える機能処理ルーチンであって前記携帯情報端末の外部と通信する機能処理ルーチンを呼び出す命令である場合に前記実行手段による前記プログラムの実行を停止させる停止手段とを備えることを特徴とする。

【００７７】ここで、機能処理ルーチンとはアプリケーションプログラムの実行環境に存在し、そのアプリケーションプログラムから呼び出され何らかの処理を行ういわゆるサブルーチンであり、例えばｉｎｖｏｋｅ　ｖｉｒｔｕａｌ等のライブラリ呼出命令により呼び出されるライブラリプログラムである。これにより、ダウンロードしたプログラムが携帯情報端末の外部と通信する機能を使用することを防ぐことができるようになる。これは例えばユーザの意図と関係なく通信料金が必要となる事態が生じるのを防ぐ等の意味を持つ点で有用である。

【００７８】また、前記機能処理ルーチンは前記携帯情報端末の外部へのデータ送信を行う機能処理ルーチンであることとしてもよい。これにより、携帯情報端末からの機密情報の流出を防ぐことができるようになる。また、本発明に係るプログラム実行制御装置は、携帯情報端末に搭載され、複数の命令からなるプログラムを取得して実行するプログラム実行制御装置であって、通信路からプログラムを取得する取得手段と、取得したプログラムを実行する実行手段と、実行中のプログラムが次に実行しようとする命令を監視し、前記命令が前記携帯情報端末が備える機能処理ルーチンであって前記携帯情報端末が備える出力デバイスからのデータ出力を行う機能処理ルーチンを呼び出す命令である場合に前記実行手段による前記プログラムの実行を停止させる停止手段とを備えることを特徴とする。

【００７９】これにより、ダウンロードしたプログラムが携帯情報端末のディスプレイにパスワード等の秘密の情報を表示する等の出力動作を行うことを防止することができる。また、本発明に係るプログラム実行制御装置は、携帯情報端末に搭載され、複数の命令からなるプログラムを取得して実行するプログラム実行制御装置であって、通信路からプログラムを取得する取得手段と、取得したプログラムを実行する実行手段と、実行中のプログラムが次に実行しようとする命令を監視し、前記命令が前記携帯情報端末が備える機能処理ルーチンであって前記携帯情報端末が備える入力デバイスからのデータ取得を行う機能処理ルーチンを呼び出す命令である場合に前記実行手段による前記プログラムの実行を停止させる停止手段とを備えることを特徴とする。

【００８０】これにより、ダウンロードしたプログラムが携帯情報端末に備えられたマイクを通じてデータを取得して盗聴を行う等のデータ取得動作を行うことを防止することができる。また、前記プログラム実行制御装置はさらに、前記停止手段によって前記プログラムの実行が停止した場合に、停止した旨をユーザに通知する通知手段を備えることとしてもよい。

【００８１】これにより、ユーザはダウンロードしたプログラムの実行が停止されたことを知ることができるようになる。また、前記プログラム実行制御装置はさらに、前記停止手段によって前記プログラムの実行が停止した場合に、ユーザによる入力を受け付けて前記入力に応じて停止を解除する停止解除手段を備えることとしてもよい。

【００８２】これにより、ユーザはプログラムの実行が停止された場合にその停止を自己の判断によって解除することができるようになる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係るプログラム実行装置３００等の構成図である。

【図２】プログラム実行装置３００を備える携帯電話機とダウンロード対象のオブジェクトプログラムとの関係を示す図である。

【図３】機能ＩＤテーブルのデータ構造及び内容例を示す図である。

【図４】オブジェクトプログラムに付加される実行時使用機能情報のデータ構造及び内容例を示す図である。

【図５】使用禁止テーブル３０４のデータ構造及び内容例を示す図である。

【図６】メモリ内の領域の分類を示した図である。

【図７】個人情報の内容の具体例を示す図である。

【図８】プログラム実行装置３００がダウンロードしたオブジェクトプログラムを解釈実行する際における処理手順を示すフローチャートである。

【図９】使用機能監視部３０２による監視処理を示すフローチャートである。

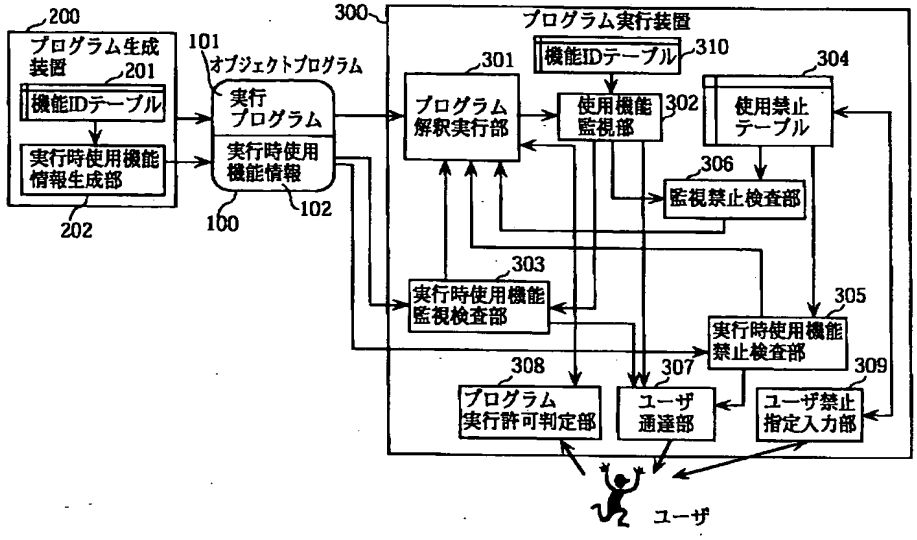
【図１０】解釈実行停止処理を示すフローチャートである。

【図１１】ユーザ通達部３０７の制御によりディスプレイに表示される画面の例を示す図である。

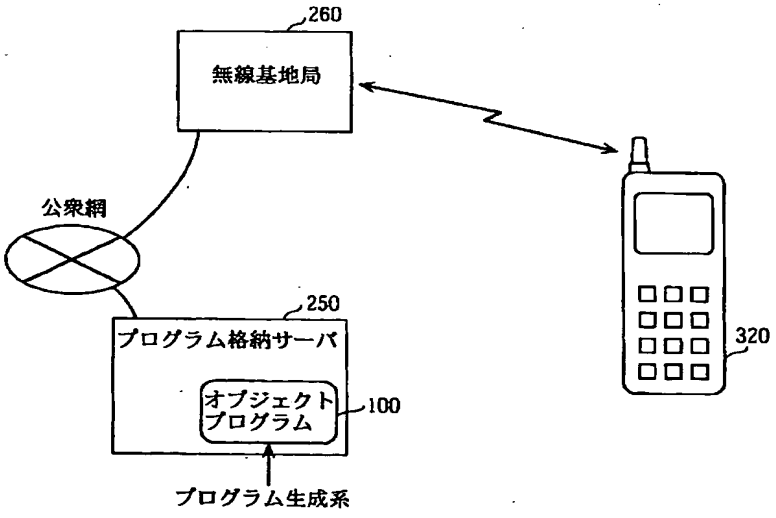
【図１２】ユーザ禁止指定入力部３０９が携帯電話機のディスプレイに表示するよう制御する使用禁止機能選択

画面を示す図である。
【図１３】メモリ内に個人情報であるデータと個人情報以外であるデータがフラグによって識別可能となるように格納されている例を示す図である。
【符号の説明】
１００　オブジェクトプログラム
１０１　実行プログラム
１０２　実行時使用機能情報
２００　プログラム生成装置
２０１　機能ＩＤテーブル
２０２　実行時使用機能情報生成部
３００　プログラム解釈実行装置
＊３００　プログラム実行装置
３０１　プログラム解釈実行部
３０２　使用機能監視部
３０３　実行時使用機能監視検査部
３０４　使用禁止テーブル
３０５　実行時使用機能禁止検査部
３０６　監視禁止検査部
３０７　ユーザ通達部
３０８　プログラム実行許可判定部
３０９　ユーザ禁止指定入力部
３１０　機能ＩＤテーブル

【図１】



【図２】



【図４】

実行時使用機能情報

500	501	502
	機能ID	フラグ
	0x0001	0x00
	0x0002	0x01
	0x0003	0x00
	0x0004	0x01
	0x0005	0x00
	⋮	⋮

【図３】

400 機能IDテーブル

機能ID (401)	ライブラリ番号 (402)
0x0001 (無線I/Fへのデータ出力)	6
0x0002 (ディスプレイへのデータ出力)	7
0x0003 (音声出力回路へのデータ出力)	8
0x0004 (無線I/Fからのデータ入力)	32
0x0005 (ボタンからのデータ入力)	33
⋮	⋮

【図５】

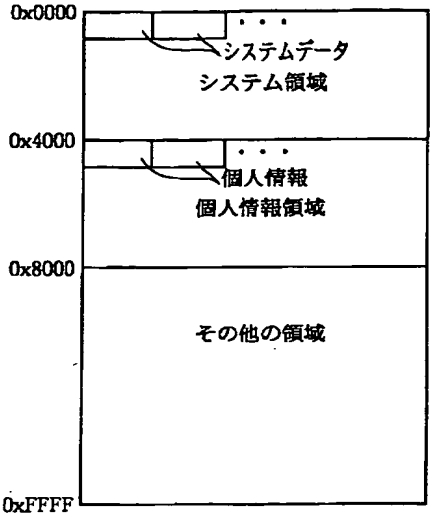
600 使用禁止テーブル

機能ID (601)	フラグ (602)
0x0001 (無線I/Fへのデータ出力)	0x00
0x0002 (ディスプレイへのデータ出力)	0x01
0x0003 (音声出力回路へのデータ出力)	0x01
0x0004 (無線I/Fからのデータ入力)	0x00
0x0005 (ボタンからのデータ入力)	0x01
⋮	⋮
0x0101 (個人情報領域からのデータ読出)	0x00
0x0102 (システム領域からのデータ読出)	0x00
0x0201 (個人情報領域へのデータ書込)	0x00
0x0202 (システム領域へのデータ書込)	0x00
⋮	⋮

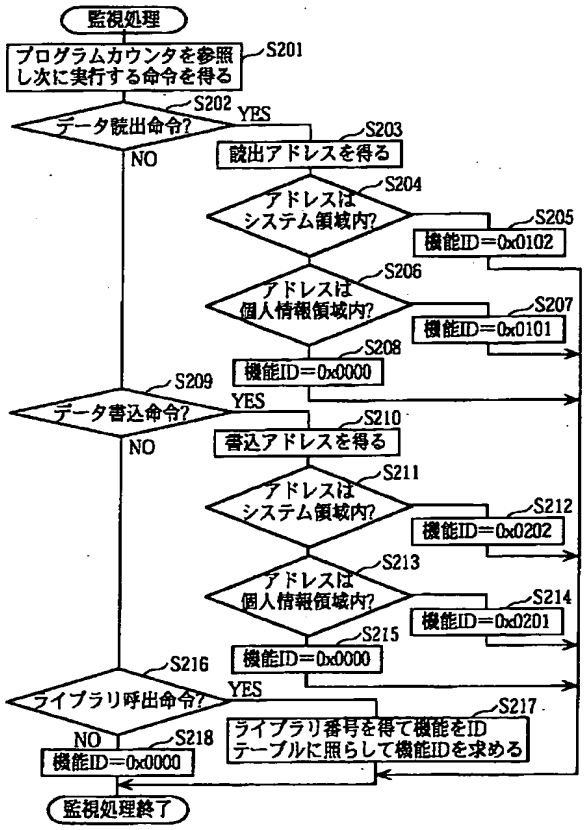
【図７】

- 人物名
- 電話番号
- 住所
- メールアドレス
- 伝言メモ
- 機器の設定、例えば、携帯電話を例にすると、
  - 着信音量
  - 通話音量
  - 着信通知の設定(着信音か、バイブレータか、あるいは別の手段か)
  - 着信時に演奏されるメロディ
  - アラーム使用時刻
  - 課金状況
  - 機器の使用時間
  - 留守番電話にしているか否か
  - FAXを受けられるか否か

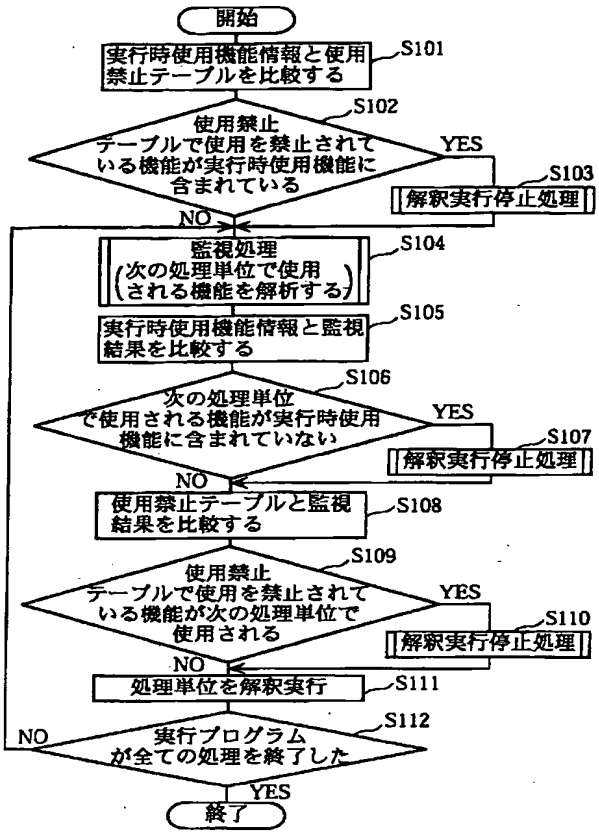
【図６】



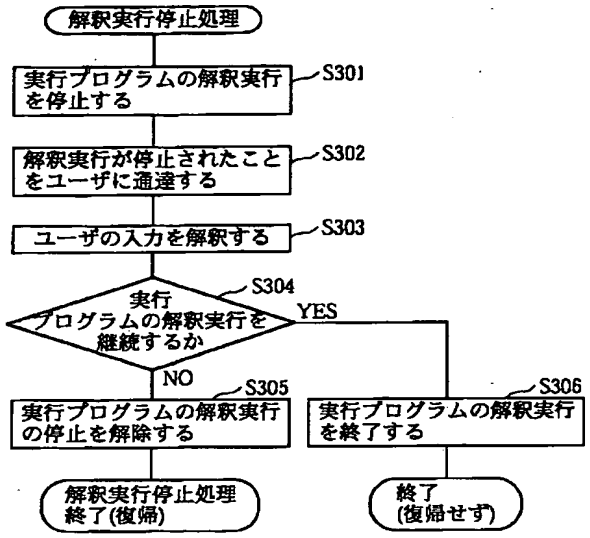
【図９】



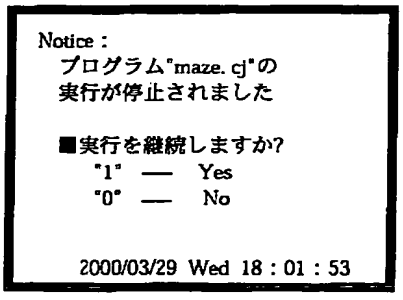
【図８】



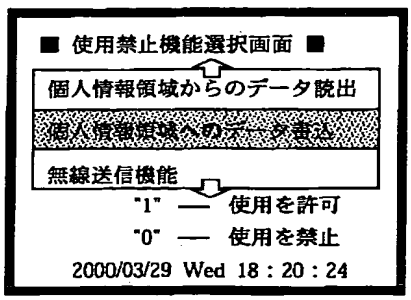
【図１０】



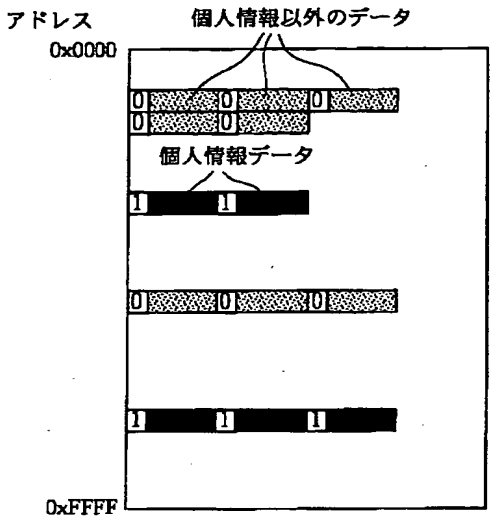
【図１１】



【図１２】



【図１３】



フロントページの続き

(72)発明者　富永　宣輝
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　春名　修介
大阪府門真市大字門真1006番地　松下電器産業株式会社内

Ｆターム(参考)　5B017 AA08 BB06 CA15
5B076 BB06 FA00 FB02